THE REGULATION OF HACKTIVISM IN CONTEMPORARY SOCIETY: PROBLEMS AND SOLUTIONS

By Vasileios Karagiannopoulos

Submitted in fulfilment for the degree of Doctor of Philosophy, School of Law, University of Strathclyde, 2013

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Abstract

This thesis focuses on the issue of regulating legally ambiguous political activities online, what is more specifically characterised as hacktivism or electronic civil disobedience. This work aims to discuss whether these political activities, despite their prima facie illegal nature, also constitute an important aspect of democratic political expression online that can be moral and entail politically useful elements that eventually make it distinct from purely criminal acts and thus deserving of a different regulatory approach.

After identifying and assessing the special characteristics of hacktivism as a potentially moral political activity, the thesis attempts to show how the current regulatory approach, which mainly employs cybercrime legislation and criminal justice processes in order to regulate hacktivist actions can often produce not only unjust, but also inefficacious results. Essentially, the analysis highlights the ways that the currently adopted approach compromises, not only the civil liberties and rights of activists and generally users, but also, the promotion of online security and even leads to the radicalisation of politically active users.

Based on these arguments, the ultimate goal of the thesis is to develop alternative ways that the current regulatory approach can be improved and further supplemented in order to gradually shift towards a more deliberative and collaborative mode. The suggested improvements and ultimate shift of regulatory rationales entails the more active engagement of new regulatory agents and also the use of additional, new tools and processes. Through this analysis, this work finally aims to show how the synergy of all the existing and additional regulatory factors can eventually produce more legitimate regulatory solutions for hacktivism through the adoption of a symbiotic and cooperative, rather than conflict-based regulating rationale.

Acknowledgements

It feels very strange writing those words, the last part of the thesis before going to print. There were many times I was thinking about this moment and it always felt so distant, as if it would never come. Now that this whole journey is drawing to a close I feel, naturally, very happy, but also melancholic, doing a retrospective of the past years that were very adventurous in good and bad ways.

Throughout this process, many people have helped in their own ways and are part of this work. Without their support, advice, belief in me and friendship I would not have made it. I especially like to thank everyone in the Law School for standing by me, supporting me practically and psychologically and giving me the strength to reach the end of the road. I cannot but make a special mention to my supervisors, Professor Donald Nicolson, Dr Konstantinos Komaitis and Dr Benjamin Farrand, who, each in their own way contributed to my personal development as an academic and to the shaping of this thesis. I would also like to thank all my friends for enjoying the good times with me and giving me courage when the times were hard.

This thesis is also dedicated to all those embracing new technologies in order to express themselves artistically and politically in innovative ways, challenging our perceptions and forcing us to reconsider our settled ways and beliefs. It is the creativity of these people that inspired me and provided me with a thesis topic that I felt passionate enough about to dedicate all these years to exploring.

Last but not least, this work is dedicated to my parents, my mother who, sadly, did not have the chance to see this day, but is always with me and my father who always did everything in his power so that I can be who I am and be where I am today.

TABLE OF CONTENTS

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 1

HACKTIVISM AND RELEVANT REGULATORY CHALLENGES: SETTING THE SCENE

The Internet has become part of our everyday lives. The various phenomena and developments in the online world express important human needs and desires, demonstrating the growing importance of the 'virtual', cyberspace dimension and its inevitable blending with the offline world in constituting the sum of what we experience. Consequently, almost every dimension of our lives has developed an online aspect, from commerce and crime to public services, political activity and even dating.

This thesis will analyse one of the most ambiguous aspects of online political activity: the practice of transgressing cybercrime laws with the purpose of symbolically expressing dissent in the online environment. Such activities have been dubbed hacktivism due to the use of software tools for facilitating the political symbolic expression online, usually through unauthorised modifications on webpages. The, prima facie at least, illegal nature of hacktivism has given rise to wide discussion in relation to its moral justifiability and its potential harmfulness for networks and the interests of the networks' operators and users. Recently, these activities have become prolific, as has the discussion on how they should be treated. The persisting existence of hacktivism as a political practice in parallel with the development and shaping of cyberspace, and the great controversy as to the nature and the treatment of such political phenomena, were the core reasons that motivated this thesis. Moreover, despite the existence of socio-political assessments of hacktivism, there has not been an extensive and deeper legal and regulatory analysis of these activities. Consequently, another motive for this thesis is to provide the first in-depth legal and regulatory analysis of hacktivism. Furthermore, this research will attempt to identify the potential problems of the existing approach for user rights and cybersecurity and eventually suggest ways for responding more appropriately to the contemporary needs for online security, but also to the potentially special nature and role in online politics that hacktivism can have.

In order to understand how hacktivism has come about, its importance and its role and, consequently, also demonstrate the reasons that an analysis of the phenomenon seems capable of justifying such an extensive analysis, it is necessary to provide some background information in relation to the concept of regulation, but mainly regarding the Internet, the power relations influencing the regulation of online phenomena and the role of hacktivism in these processes. This discussion will allow the reader to realise how the Internet has gradually developed as a regulable space with important power conflicts taking place and also understand the nature of hacktivism and its important role in cyberspace politics.

1. The concept of regulation: from state to networks

1.1 Defining regulation

Before proceeding to discuss the Internet and its regulation, the concept of regulation as will be perceived in the thesis will need to be defined. Regulation has eluded a concrete form and, thus, also a concrete definition. Definitions have indeed ranged from, narrow, state-centred ones, where regulation is perceived as the 'deliberate attempts by the state to influence socially valuable behaviour which may have adverse side-effects by establishing, monitoring and enforcing legal rules,'[1] to broader ones, encompassing 'all forms of social control, intentional or not originating from social institutions even beyond the state'.[2]

The thesis will follow a broader interpretation of regulation in acknowledgment of current trends in regulation theory that broaden the scope of regulatory processes by including new actors and ways of perceiving regulation, both online and offline.[3] Although,

[1] Brownen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, Cambridge 2007) 3.

[2] ibid 4.

[3] See Clifford Shearing and Jennifer Wood, 'Nodal Governance, Democracy, and the New 'Denizens'' (2003) 30 Journal of Law and Society 400; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, New York 1995); Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a" Post-Regulatory" World' (2001) 54 Current Legal Problems 103*;* See also Internet-related networked regulation theories Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic books, New York 1999); Andrew D. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge London 2007); Joel R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory Law Journal 911.

traditionally, discussions on regulation had focused on the state and its rule-making and coercive power, the gradual complexity and diversity of socio-economic affairs, exacerbated by new technologies and the general evolution of societies and markets, have made the regulatory weaknesses and deficiencies of the state, such as issues of jurisdictional reach and enforcing specialised information, even more obvious.[4] As has been argued, governments, generally operating on top-down principles, do not allow entrepreneurship in resolving problems and are inefficient, slow and impersonal.[5] Consequently, these deficiencies highlight the need and inevitability of engaging more regulatory agents in the process that will be able to resolve these problems, with the state steering their efforts at a distance, but not governing directly.[6] This in turn has led to the wider acceptance and development of broader regulatory accounts that now include new stakeholders, institutions and modes of action that can potentially deal with the novel challenges more efficiently and/or justly.[7]

'Nodal',[8] multi-actor regulation allows for more informed understanding of the complexities introduced by each problematic and through the subsequent fragmentation of power and control, which promotes more efficient and more democratically accountable solutions through the interplay of various regulatory actors.[9] A network of regulating actors, thus, assures that more context-specific regulatory options spring out of the interaction of the various competing and cooperating network nodes, remedying any inefficiencies and injustices in the process.[10]

[4] See Julia Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 2;For an extensive analysis on the failures of the state see also Ian Loader and Nigel Walker, *Civilizing Security* (Cambridge University Press, Cambridge 2007).

[5] Clifford Shearing, 'Reflections on the Refusal to Acknowledge Private Governments' in Jennifer Wood and Benoit Dupont (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge 2006) 23.

[6] ibid 23.

[7] Scott Burris, Michael Kempa, and Clifford Shearing, 'Changes in Governance: A Cross-Disciplinary Review of Current Scholarship' (2008) 41 Akron Law Review 1, 5.

[8] 'Nodal governance focuses on the nodes-the institutions of governance-in systems of networked power: their internal constitutions, their cultures, their resources, and the strategies they use to amass and project power. A "node" is any formal or informal institution that is able to secure at least a toe-hold in a governance network [...] from government entities, to foundations and NGOs, to street gangs.' ibid 25-6.

[9] Black, 'Critical Reflections on Regulation' (n 4) 3-4.

[10] Jennifer Wood, 'Research and Innovation in the Field of Security: A Nodal Governance View' in Jennifer Wood and Benoit Dupont (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge 2006) 218; Jennifer Wood, Clifford Shearing, and Jan

This conflict regarding the influence of traditional models and the need, or the inevitability, of including more actors came to the fore more saliently regarding the advent of the Internet, which constituted a new cluster of interconnected networks, the regulation of which was being formulated along with its development. With its popularisation, the Internet constituted a new space for multiple phenomena that required regulation, such as criminality, speech or commercial exchanges and, thus, a similar discussion regarding regulatory networks developed in order to reflect the power balances and the new regulatory actors and tools that were available in this technological space. In order to understand these online power conflicts that impact on the regulation of Internet phenomena and the role of hacktivism in these conflicts, a discussion on the development of the Internet and its power relations will follow.

1.2 The modern networks

Contemporary societies increasingly rely on interconnected informational networks, the Internet being one of the most prominent, and with the focal point being information, which is more than ever before shaping the global economic, political and cultural landscape, theorists suggest we are currently living in an era of networked, information-based societies.[11] The gradual development of the Internet has actually transformed it from a communications tool to a social space of interlinking networks - a cyberspace- where 'words, human relationships, data, wealth, and power are manifested by people using computer-mediated communications technology.'[12] This analysis will use the terms, Internet and cyberspace, interchangeably.

Castells describes network society as:

Froestad, 'Restorative Justice and Nodal Governance' (2011) 35 International Journal of Comparative and Applied Criminal Justice 1, 1.

[11] Various criteria have been used for identifying what is new in the information society, from technological and economic to occupational, spatial and cultural. Frank Webster, *Theories of the Information Society* (3rd edn, Routledge, London 2006) 8-9.

[12] 'Cyberspace[...]is the name some people use for the conceptual space where words, human relationships, data, wealth, and power are manifested by people using computer-mediated communications technology.' Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (The MIT Press, Cambridge (MA) 2000) cited in Suart Biegel, *Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace* (The MIT Press, London 2003) 33.

> [A]society whose social structure is made of networks powered by microelectronics-based information and communication technologies. [...] A network is a set of interconnected nodes. A node is the point where the curve intersects itself. A network has no center, just nodes. Nodes may be of varying relevance for the network. Nodes increase their importance for the network by absorbing more relevant information, and processing it more efficiently.[13]

The advent of new technologies, such as the Internet, has increased the importance of information and has further empowered various non-state actors that are able to produce and process it, such as corporations or even plain users and, thus, governance gradually became a more fragmented process, with power distributed to more, non-state actors. Internet theorists started discussing the role of hierarchical, law-based models and their weaknesses in regulating cyberspace efficiently and legitimately, eventually suggesting more decentralised self-regulatory approaches as more efficient and politically legitimate.[14] Others like Goldsmith still maintained a belief in the predominant role of law and its regulatory potential, arguing, however, that whenever laws were challenged by the difficulties posed by the global and technologically novel nature of the Internet, new actors and tools, such as online intermediaries, could feature in the process of regulating.[15] Other theorists, such as Reidenberg and Lessig, argued more explicitly for the need to engage actively with new regulatory actors and tools, mainly through the use of technology as an architectural control in the technological networks.[16] As Lessig explains regarding online regulation 'norms constrain through the stigma that a community imposes; markets constrain through the price that they exact; architectures constrain through the physical burdens they impose; and law constrains through the punishment it threatens.'[17] The role of these regulatory modalities will be discussed extensively during those chapters which critique the current regime and explore alternative solutions.

[13] Manuel Castells, 'Informationalism, Networks, and the Network Society: A Theoretical Blueprint' in Manuel Castells (ed), *The Network Society: A Cross Cultural Perspective* (Edward Elgar Publishing Ltd, Cheltenham, 2004) 3.

[14] David Johnson and David Post, 'Law and Borders-the Rise of Law in Cyberspace' (1995) 48 Stanford Law Review 1367; David Post, 'Anarchy, State and the Internet' (1995) 3 Journal of Online Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943456> accessed 18 December 2012.

[15] Jack L. Goldsmith, 'Against Cyberanarchy' (1998) 65/4 The University of Chicago Law Review 1199.

[16] Lawrence Lessig, *Code v.2.0* (Basic Books, New York 2006) Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 533.

[17] Lessig, *Code v.2.0* (n 16) 124.

The realisation of the Internet’s potential for decentralisation of power rendered multi-actor forms of regulation more relevant and put informational networks at the centre of discussion in relation to how political power is generated, shaped and challenged. Moreover, with the Internet, the constitutive element of power also shifted, with information becoming the predominant source and resource of power.

1.3 Information and power in the networks

Information has been crucial for economic and socio-political development even since the formation of the nation state.[18] However, the contemporary technological developments, with the Internet and digital technologies prominent among them, have dramatically reinforced and emphasised its role. Information, apart from being the life-blood of communications networks, is essential also because it generates knowledge, which inevitably leads to empowerment, since, as Foucault says, ‘it is not possible for power to be exercised without knowledge, it is impossible for knowledge not to engender power.’[19] Inevitably, power is increasingly embedded in information technologies, forming a new social paradigm, which Castells names ‘informationalism’.[20] Informationalism expresses the subsumption and subordination of the previous industrialisation processes and the focus on energy generation to the ’augmentation of the human capacity of information-processing and communication made possible by the revolutions in microelectronics, software, and genetic engineering.’[21] A natural consequence of this change, as one of the first hacktivist groups, the Critical Art Ensemble (CAE), highlights, is that the nature of power has also radically changed: ‘[D]isconnected from spatial notions of state and traditional space-related attachments, power has now migrated to the immaterial, information networks, with resistance inevitably following’.[22] This realisation is also in accord with the Foucauldian view that wherever there is power, there will be a form of counter-power opposing it.[23]

[18] Webster (n 11) 210-11.

[19] Michel Foucault, 'Prison Talk ' in Colin Gordon (ed), *Power/Knowledge* (Harvester, Brighton 1980) 52.

[20] Manuel Castells, *Information Age, Economy, Society and Culture* (Blackwell, Oxford 1996) 17 cited in Webster (n 11) 101.

[21] Castells, 'Informationalism, Networks, and the Network Society’ (n 13) 8-9.

[22] Critical Art Ensemble, *'Electronic Disturbance'* (Autonomedia, New York 1993) 111-2.

[23] Michel Foucault, *The Will to Knowledge: The History of Sexuality* (Penguin, London 1998).

Power is, thus, related to information management even more directly than in previous eras and moderating or liberating information flows becomes the centre of attention for factions and actors vying for control of the various aspects of society. The importance of information is reflected in the discussions that focus on the regulatory potential of information technologies, hardware and software, which Lessig has characterised as 'code', the building blocks of what constitutes our Internet experience.[24] Code regulates how information is generated and communicated, how it can be restricted, through filtering for example, or how it could be protected through encryption. For Lessig, technology is as important for regulation online, as law is offline, since, in the malleable virtual environment of cyberspace, hardware and software can be very effective in shaping our online environment, managing behaviours and defining user capabilities, with a regulatory, but also a deregulatory, potential.[25] For example, in the same way that code-makers can help enforce a legal ban on a specific type of information, such as child pornography, they can develop encryption software that will allow the distribution of such information despite the authorities' prohibitions.[26]

Considering the predominant role of information, conflicts for managing information per se, but also the tools for regulating information-production and distribution, have generated many power struggles between actors that attempt to increase their control or facilitate as much liberation of information as possible.[27] These power actors interact and compete within a network of power relations, subsequently establishing and influencing the dominant societal values through the interplay between them and set the backdrop, where all political conflicts take place.[28] It is now time to establish an understanding of how power and resistance actors interact on the Internet and the role of hacktivism in these interactions.

[24] Lessig, *Code v.2.0* (n 16).

[25] ibid 24; Tim Wu, 'When Code Isn't Law' (2003) 89 Virginia Law Review 103, 104-6.

[26] Wu (n 25) 104-6.

[27] A typical example is the conflict of copyright infringement and piracy. This conflict engages not only the studios and the users, but also private online companies, states, international organisations and consumer organisations.

[28] Castells (n 13) 24-5, 30. For Foucault, power is not only decentralised to many people, but also relational and ubiquitous, as it exists within all deliberate, multiple human interactions, instead of just being focused on one agent as a quantum of force to be exercised hierarchically. See Mark G.E. Kelly, 'The Political Philosophy of Michel Foucault' (Taylor & Francis e-Library, 2009) 37-8.

1.4 The shifting power balance in cyberspace

In order to better understand the power structure of the Internet, some details of its birth and development are required. Being initially a US military-related project for facilitating the decentralisation of communications, the Internet was introduced to the wider public in the mid-90s through a privatisation process. At the beginning, use was limited to primarily research networks and discussion forums, before being adopted by commercial and governmental websites. Gradually educational research, communication and, later, commercial activities started to evolve online, taking advantage of the openness and innovation potential of the technologies by which the Internet was created. More particularly, Internet communications were based on packet switching technologies and protocols, such as the transmission control protocol/internet protocol (TCP/IP), which broke information into packets and transmitted them over the network indiscriminately, thus, preserving the neutrality of the network towards the transmitted information.[29] This core infrastructural element of non-discrimination between the various types of information circulated online allowed new hardware and software to develop and gave rise to new types of communication and services by taking advantage of the potential for innovation this neutrality allowed.[30]

However, according to Murray, the birth of the modern Internet is to be attributed to two events - a technological invention - the creation of the World Wide Web (WWW) technology - and a deregulating act - the free distribution of this technology for promoting compatibility and interoperability online.[31] WWW technology enabled the creation of a library of information online in the form of pages that could be accessed under specific addresses and the use of web browsers that enabled the transition from one address to the other.[32] The combination of these technologies transformed the Internet into a more

[29] TCP/IP protocols fragment information into smaller data packets and provide them with the address they would go to. These packets could take variable routes to reach their final destination. Andrew D. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge, London 2007) 67-8.

[30] For the importance of the net neutrality principle for innovation and counterarguments see: Tim Wu and Christopher S. Yoo, 'Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate' (2007) 59 Federal Communications Law Journal 575.

[31] Murray (29) 71-2.

[32] The World Wide Web is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view webpages that may contain text, images, videos, and other

functional and user-friendly milieu of interconnected networks and enabled its extensive commercialisation and popularisation. The above technologies (TCP/IP, WWW) and the willingness of the state to delegate important regulatory tasks to self-regulating private actors[33] resulted in the Internet developing mostly with principles of openness and self-management that made it publicly appealing and, thus, facilitated its uptake.

The gradual technological evolution of the Internet led to a significant twist at around the turn of the century with the introduction of a new category of online platforms and software applications, which signified a transition to a second, information-richer generation of the Internet: Web 2.0, as it was commonly named. The main focus of Web 2.0 applications, such as blogs, wikis or social networks, is to enable users to produce their own content in a more personalised format, which entailed a one-to-many production and distribution of information and more dynamic interaction between users. This interaction and potential for collaboration simultaneously empowered civil society and provided it with additional tools for influencing the shaping of the new information-based society. Web 2.0 coincided with the popularisation of bandwidth Internet services, which greatly increased the speed of the network connections, even for home users, allowing a quantitative and qualitative increase in the information that could be produced and exchanged.

However, the initial openness and focus on privacy and free information exchanges was and is increasingly challenged, especially after the medium's popularisation, by many corporations, governmental authorities and even international organisations that have profit-making and power-yielding interests in controlling information online. The advent of various groups of actors with conflicting interests and the gradual commercialisation of the Internet inevitably led to concerted efforts to counteract the openness of the networks through the creation of information-controls. These ranged from technical, such as censorship software or technologies that gave priority to certain types of information, or legal, such as prohibitions to copyrighted file-exchanges.

multimedia, and navigate between them via links. Wikipedia, 'World Wide Web' <http://en.wikipedia.org/wiki/World_Wide_Web > accessed 29/05/2012.

[33] Examples would be the management of the domain name system by the Internet Corporation of Assigned Names and Numbers (ICANN) or the Internet Engineering Task Force (IETF), which was responsible for setting technological standards and protocols for cyberspace.

As Lessig, argues, the initial phase of openness was too inconsistent with the general power flows to survive unchallenged.[34] In his words:

> [A]s these cultures [openness vs control] came into conflict, real-space law quickly took sides. Law worked ruthlessly to kill a certain kind of online community. The law made the hackers' behavior a "crime," and the government took aggressive steps to combat it. A few prominent and well-publicized cases were used to redefine the hackers' 'harmless behavior' into what the law would call "criminal." The law thus erased any ambiguity about the 'good' in hacking.[35]

The introduction of the user-content-based era was also stigmatised by grave political events – in particular, the major terrorist attacks in western capitals, New York, London and Madrid, which provided fertile ground for a more generalised paradigm shift towards control. States became much more active in managing information either through extensive legislation or indirectly through influencing online companies that could exert control over information, such as Internet Service Providers (ISPs) or content providers and software developers.[36] Therefore, the need to promote safer information exchanges for e-commerce to blossom, in addition to the fear of terrorism naturally reinforced the trends of control, where the state, especially as far as online security, information control and political activity are concerned, became much stricter, passing new laws, such as the PATRIOT ACT in the US or the Terrorism Act of 2006 in the UK.[37] These laws have intensified the criminalisation of controversial political acts and simultaneously increased the surveillance capabilities of the authorities, inevitably also engaging the state more actively in the process of securing cyberspace by increasing technological use in addition to legislative controls. [38]

On the other hand, the Internet's malleable technological nature, simultaneously guaranteed the subverting of all sorts of controls, legal or technological. Code enables deregulation[39] and technological solutions could prove less efficient in regulating online

[34] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, New York 1999) 194.

[35] ibid.

[36] Ch 4, Part 4. The role of private actors.

[37] See detailed analysis in Ch 4, Part 3.3.4 Hacktivism and the link with cyberterrorism.

[38] See examples in Rebecca Mackinnon, *Consent of the Networked:The Worldwide Struggle for Internet Freedom* (Basic Books, New York 2012) 76-8.

[39] Joel R. Reidenberg, 'States and Internet Enforcement' (2004) 1 University of Ottawa Law & Technology Journal 216, 235-6.

behaviours, since techniques of bypassing restrictions can be easily found online and are massively employed.[40] Castells also argues that no power elite can firmly control the setting of norms and goals for the informational networks, without these standards being challenged and no power that can eliminate the synergies between various actors that undermine the efforts of others, since they are all engaged in a constant interplay for increasing their own influence.[41] Information controllers, thus, try to preserve and expand their influence and so do counter-control factions.[42] On the one hand, there iaremainly states and corporations, which would like to gain more control over information and, consequently, over most of the socio-political and economic processes. On the other hand, counter-power is usually constituted by groups of users, activists, Non-Governmental Organisations (NGOs) and other collectives, which desire the liberation of information from the controlling factions and the promotion of creation, use and distribution of it by the online communities.[43]

These balances are not absolute and in various cases corporations could side with the public against overly restrictive laws or states could even impose sanctions on companies, for example, for user-privacy violations. In an environment of a constant tug-o-war, competing networks win and lose legal and technological battles for imposing their views, shaping the Internet's normative and practical realities through their synergies and conflicts.[44] As Klang argues, 'the Internet is used for every conceivable form of communication and it is therefore only natural that it should be used as an infrastructure for protest and civil disobedience'.[45]

[40] Biegel (n 12) 210; Mathias Klang, 'Disruptive Technology: Effects of Technology Regulation on Democracy' (DPhil Thesis, Goeteborg University 2006) 39.

[41] Castells, 'Informationalism, Networks, and the Network Society' (n 13) 33.

[42] Kelly (n 28) 49.

[43] Even though these examples generally characterise the two poles of power and resistance, coalitions between power actors change. An example would be corporations, such as Google, which joined users against governmental legislative propositions, such as the Stop Online Piracy Act (SOPA) and even with states joining users and corporations in promoting speech in authoritarian regimes, such as the collaboration of western political forces, citizens and Twitter in the case of Iranian political unrests in 2009.

[44] 'As a political milieu, a network culture looks more like a permanent battlefield than like a neo-socialist utopia. It is the plane over which battles for market shares and for the determination of public opinions are fought' Tiziana Terranova, *Network Culture: Politics for the Information Age* (Pluto Press, London 2004) 154.

[45] Klang (n 40) 64.

1.5 The role of hacktivists as hacker/political entities of counterpower

Within these power conflicts hacktivism is a natural development. The two constitutive elements of hacktivism, the activist and the hacker, both used technology in deregulatory ways, from facilitating political organisation and communication of resistance speech online and offline to using technologies as expression or for bypassing restrictions. More particularly, the hacker community, from which hacktivism springs, is intrinsically linked to the resistance potential of the Internet technologies, as hacking has originally meant 'the making use of technology in an original, unorthodox and inventive way'[46] and did not relate solely to illegal acts, as it predominantly is today; or better yet, the activities perpetrated then, such as software modifications, were not considered criminal. Initially, hackers were mostly those who focused on discovering new technological uses and advancing user knowledge and capabilities by sharing information and by cooperating towards innovation. However, with the gradual spread of digital technologies and the popularisation of the Internet, hackers also increased exponentially, with many of those eventually using their skills to manipulate hardware and software for malign, criminal purposes.[47]

By observing the dominant practices and perceptions of, at least, the initial hacker communities, however, Levy managed to distil certain principles that defined hacker social perceptions and also highlight their political potential. The principles of the 'hacker ethic'[48] relate to promoting meritocracy, anti-authoritarianism, freedom of information and optimism for the life-improving potential of technology and the positive effects of computerisation.[49] Despite hacker values having originated from the first, purely innovative community of programmers, they have become an integral part of the wider Internet user community today as indicated by the passion with which users converge to protest against phenomena of censorship and authoritarian control of the Internet. The examples are

[46] Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (Routledge, London 2004) 5-6.

[47] For details on the development of the hacker movement and its gradual transition from purely benign programming and 'pranksterism' to more criminal activities, see ibid 9-12.

[48] Steven Levy, *Hackers: Heroes of the Computer Revolution* (Bantam Doubleday Dell, New York 1984).

[49] The five principles as articulated by Levy are: '1) All information should be free, 2) mistrust for authority and promotion of decentralization, 3)judgement should be based on hacking skill and not physical, class or other social criteria, 4)the belief that computers can create art and beauty and 5)that they can change life for the better.' ibid 40-5.

numerous, from users sharing information online during Internet shut-down, as was done in Egypt during the protests against former President, Hosni Mumbarak, to organising mass protests against privacy-compromising copyright bills, such as the Stop Online Piracy Act (SOPA) in the US. Hacktivists, originating also from programmer or hacker communities or user collectives, adopt and promote the above hacker principles as part of their general political agenda that inevitably subverts information control efforts.

On the other hand, hacktivists also express various new tendencies in contemporary activist politics. Since information is a source of power and networks of power rely on the integrity of information and unhindered information exchanges, political organisation and the tactics of resistance also change to reflect these developments. The global proliferation of information in combination with a disappointment in more traditional mainstream political tactics, has led many political collectives to become increasingly devoted to universal political issues (economic crisis, ecology, anti-war) and to the promotion of political diversity and direct participation.[50] Moreover, many activist groups, especially those organised online, such as hacktivist collectives, do not demonstrate the concreteness and consistent membership of the past, party-based movements. Instead, cyberpolitical movements take the forms of fluid collectives, 'mobilisations' with ideologically diverse participants, who mostly converge to fight for specific goals, and where solidarity and political sensitisation are not pre-existing characteristics, but also aims and products of these mobilising initiatives.[51]

In terms of tactics, political activism has also turned towards more informal and countercultural methods and goals. The current era is characterised as one of 'meta-politics', where political activists have shifted their focus from parliamentary democracy and capturing power through party politics.[52] Consequently, many activist groups have

[50] Tim Jordan, *Activism!: Direct Action, Hacktivism and the Future of Society* (Reaktion Books, London 2002) 46, 50. One example is the World Social Forum, formed in 2001 in Porto Allegre, encompassing thousands of people with different political backgrounds and operating as an open, deliberative space coordinating global action. Anastasia Kavada, 'The Internet and Decentralized Architectures', in Athina Karatzogianni (ed), *Cyberconflicts and Global Politics* (Routledge, London 2009) 190-1; Jeffrey S. Juris, 'Networked Social Movements: Global Movements for Global Justice' in Manuel Castells (ed), *The Network Society: A Cross-Cultural Perspective* (Edward Elgar Publishing Ltd, Cheltenham 2004) 341.

[51] Robert S. Jansen, 'Populist Mobilization: A New Theoretical Approach to Populism' (2011) 29 Sociological Theory 75*,* 82-3.

[52] Alain Badiou, *Metapolitics* (Jason Barker tr, Verso, London 2005).

abandoned the effort of formal, holistic social reform through the dominating of parliamentary processes and focus on circumventing unjust laws and policies and calling on injustice, local and global, through the challenging of mainstream symbols and meanings (culture jamming) and the disruption of dominant information flows.[53] Resistance factions, thus, introduce additional information by using tactics, such as 'signal distortion, graffiti on advertising posters, hijacking of corporate events, all kind of attempts at disrupting the smooth efficiency of the communication machine.'[54] These tactics reflect the difficulty for activists to compete on a level playing field, as regards producing and distributing information over networks compared to incumbent and resource-rich actors, such as states, corporate media and infrastructure-controlling multinational companies. These new tactics also focus on creating spectacular or controversial effects in order to attract the attention of the mainstream media, in addition to being reported by the activists' own media apparatuses (Indymedia, Facebook groups, Twitter feeds). The broadening of their communication opportunities through creating spectacular, mediated events, allows activists to express their dissent more effectively and widely, sensitise the public and eventually, increase the pressure on policy-makers for political change.[55]

Hacktivism embraces and constitutes a manifestation of all these characteristics. Protests are based on media projection and in order to attract attention to the protesters' causes and sensitise and engage the public in politics beyond the traditional party processes. Their hacker-related background further supports such practices, as it allows hacktivists to jam cultural and political symbols online and cause noticeable disruptions.

Hacktivist tendencies, expressive of counter-power, also reflect the intensification of power conflicts both offline and online. Responding to the increasingly intensifying cybercriminal restrictions and crack-downs on Internet expression, user privacy and hacktivists more particularly, hacktivists have also started adopting more radical and less principled tactics under the umbrella identity of Anonymous, while earlier hacktivist groups have generally retreated from illegal activity in order to avoid criminal liability in an

[53] Naomi Klein, *No Logo: Taking Aim at the Brand Bullies* (Flamingo, London 2001) 280-3. Terranova (n 44) 17.

[54] Terranova (n 44) 17.

[55] Juris (n 50) 342; The *Reclaim the Streets* movement in Britain has held many events, where thousands of people would organise a performance with dancers, jugglers and other artistic events in main street arteries to protest against ecological destruction. Klein (n 53) 312-4.

increasingly risky cybersecurity climate.[56] Having seen the role of hacktivism in the informational networks, we will now proceed to discuss the phenomenon in more detail.

2. Hacktivism: Definitions, groups and tactics

2.1 Defining hacktivism

The concept of hacktivism can and has been defined broadly and has been so excessively used in so many different contexts that it has come to connote potentially any use of digital technologies for political reasons. This indiscriminate use of the term is also one of the main problems hacktivists face today, as their actions are analogised to purely criminal or even terrorist activities.[57] This analogising also reflects the fact that both of hacktivism's constitutive narratives - hacking and activism – have gradually ended up denoting criminal or subversive behaviours.[58] Moreover, the mantle of hacktivism has been adopted by criminally-minded hackers attempting to legitimise or glorify their non-political exploits and has also been excessively and indiscriminately used in sensationalist media reports and by cybersecurity experts and government officials for many incidents of computer-systems disruption that might have a political hue.[59] However, the thesis will focus on those activities that are primarily symbolically expressive, political acts realised through illegal techniques of computer modification and network disruption that violate cybercrime laws, because these activities pose the most controversy and complexity in terms of their regulation, since they combine punishable elements of violating criminal laws with protectable politically expressive elements, such as free expression and assembly rights.

[56] Evan R. Goldstein, 'Digitally Incorrect' (*The Chronicle Review*, 03 October 2010) <http://chronicle.com/article/Digitally-Incorrect/124649/> accessed 12 August 2011;The Electrohippies Collective, 'Cyberlaw UK: Civil Rights and Protest on the Internet' (*iwar.org,* 2000)< http://www.iwar.org.uk/hackers/resources/electrohippies-collective/comm-2000-12.pdf> accessed 15 February 2013.

[57] Ch 4, Parts 2.2 The deviant 'Other' and hacktivists and 3.3.4 Hacktivism and the link with cyberterrorism.

[58] Ch 4, Part 2. The normative framework and its impact on hacktivism.

[59] Sandor Vegh, 'Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank' in Martha McCaughey and Michael D. Ayers (eds), *Cyberactivism: Online Activism in Theory and Practice* (Routledge, London 2003) 83; Alexandra W. Samuel, 'Hacktivism and the Future of Political Participation' (DPhil Thesis, Harvard University 2004) 26-8.

In an effort to narrow down the concept of hacktivism to be employed in the thesis, I would argue that 'Hacktivism is the fusion of methods of computer systems modification or reconfiguration that transgress cybercrime laws and target computer systems and networks to produce or simulate effects that confer a political message or protest a particular policy.'[60] Acts that do not violate cybercrime laws, such as website parodies, or lack a politically expressive element fall out with the scope of this thesis. Non-politically expressive acts would be more akin to plain criminality, lacking a moral political element or a link to the exercise of civil liberties, while activities that do not break laws would also fail to create a regulatory controversy that would require particular examination. The concept of hacktivism to be examined in this thesis will become clearer through the following discussion of the history of hacktivist groups and their tactics, which will constitute the focus of the following analysis. Although many groups that could be characterised broadly as hacktivist have not been included, attention has been given to specific groups/collectives that have been more popular and eloquent in their ways and which have generated interventions that entail expressive and illegal elements, thus, requiring further regulatory discussion.

2.2 Hacktivist groups and tactics

2.2.1 The first era of hacktivism and the birth of electronic civil disobedience

Hacktivist action and electronic forms of illegal, symbolically expressive protests were first articulated in the writings of the Critical Art Ensemble, an activist group focusing on general tactical media interventions.[61] CAE's writing focuses on the importance of information generation, control and distribution in the current networked economies. The main contribution of CAE to the development of hacktivism is an extensive analysis of notions ranging from electronic civil disobedience (ECD) to less expressive and more disruptive direct action tactics. CAE defines ECD as the transition of the tactics of blockage and

[60] For definitions see Samuel (n 59) 1-2.

[61] Tactical media encompasses hacktivism, but generally involves the use of new technologies in artistic projects that instead of attempting to generate grand revolutionary events, focus on producing micropolitical effects that disrupt, intervene and educate. Rita Raley, *Tactical Media* (University Of Minnesota Press, Minneapolis 2009) 1.

trespass onto the internet.[62] They submit that application of these tactics should always seek to avoid causing damage to websites that are irrelevant to the cause protested or are used for the provision of critical services.[63] CAE accept such activities could provoke sometimes unpredictable consequences and collateral damage, as they deem such occurrences inherent in social protests.[64]

Multiple tactics have indeed been used for politically expressive purposes, such as web defacements/redirects, and virtual sit-ins. Webpage defacements entail gaining unauthorised access to a webpage and making modifications that add or modify information on the webpage with or without the removal of the original data.[65] Site redirects involve getting unauthorised access into a web server and changing its address so that those accessing the site are redirected to an alternative site that is usually critical of the hacked site.[66] The virtual sit-in aims to block access to a service or a website by directing an overwhelming amount of coordinated data at the target server, which consequently slows down or crashes under overwhelming traffic. Depending on what ports are enabled on the server, these blockades can be achieved by flooding the server with a large number of emails that are beyond its capability to handle (email bomb), overloading an Internet Relay Chat channel (iRC jamming) or overwhelming the server with small data packets (ping storm).[67] Virtual sit-ins are based on the deliberate participation of protesters, rather than the deployment of compromised computers by a hacker, who can control huge networks of computers (botnets) which she has access to, without the owner's knowledge.[68] More rarely, hacktivists have even resorted to writing viral software that can spread to multiple computers and communicate political messages.

The teachings of CAE regarding ECD were put to practice by other groups that focused on such symbolic network disturbances. During, what can be called the first era of hacktivism, from the late 90s until the mid-00s, one of the most important groups was the

[62] Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas* (Autonomedia, 1996) 18.
[63] ibid 18, 24.
[64] Critical Art Ensemble, *Electronic Disturbance* (Autonomedia, New York 1993) 25, 120.
[65] Mathias Klang, 'Civil Disobedience Online' (2004) 2 Info, Communications and Ethics in Society 75*,* 77.
[66] Samuel (n 59) 10.
[67] Vegh (n 59) 85-6.
[68] Jordan and Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (n 46) 76-77.

Electronic Disturbance Theater (EDT), which was formed by a small team of four people with artist, activist and technical backgrounds. As Dominguez, one of EDT's core members argued, EDT 'attempted to translate and express the unbearable weight of physical beings into the immaterial informational channels', without any regard for technical efficiency, as their goal was not: 'to bring the enemy down, but be "effective" in side-loading information beyond the local and offering a point of focus for the communities involved'.[69] EDT did not see their activities as undercover direct action, but instead interpreted them as artistic gestures and performances combined with notions of civil disobedience, which would have to be realised publicly and openly in order to avoid prosecution.[70] Their online disobedience/performances were focused on organising virtual sit-ins, through the use of a specialised software tool, called Floodnet. Floodnet was freely available for download and essentially automated the process of reloading a webpage, thus, making virtual sit-ins more efficient.

EDT came dynamically to the fore during their support for the Zapatista struggle in Mexico in the late 90s, and even though the groups has currently disbanded, its members still participate in similar projects, with Dominguez continuing to organise many different actions to protest issues from healthcare budget cuts to US immigration policies and even police killings in Greece even after EDT disbanded.[71] His latest virtual sit-in in relation to budget cuts by the Santa Clara University, where he teaches digital arts, even invoked the threat of federal prosecution, with investigations being dropped only after a private agreement with the University, with Dominguez pledging not to employ such tactics either through or against the University.[72]

[69] Bruce Simon, 'Illegal Knowledge: Strategies for New Media Activism: Dialogue with Ricardo Dominguez and Geert Lovink' in Bousquet Marc and Wills Katharine (eds), *The Politics of Information: The Electronic Mediation of Social Change* (Altx Press 2003) 62.

[70] Goldstein (n 56); Ricardo Dominguez, 'Electronic Disobedience Post-9/11' (2008) 22 Third Text 661*,* 669-670.

[71] See: Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Jon Arquila and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND Corporation 2001) 266-7; Ricardo Dominguez, 'Electronic Civil Disobedience' (*thing.net,* undated) <http://www.thing.net/~rdom/ecd/ecd.html> accessed 16 January 2011; Ricardo Dominguez, 'Electronic Civil Disobedience in Solidarity with Greek Anarchists' (*thing.net*, 2008) <http://post.thing.net/node/2457> accessed 19 December 2011.

[72] Goldstein (n 70).

Similar tactics were also followed by another UK group, the Electrohippies, who, in Seattle during World Trade Organisation (WTO) meetings, promulgated their own protest tool and organised very successful protests against the network servicing these meeting to protest capitalist globalisation policies.[73] The Electrohippies also published a list of preconditions for using their virtual sit-in tool, ranging from providing information facilitating the traceability of protesters by the authorities, to providing prior notification to the targets and explanation of the motives and the cause of the protest.[74] However, despite the success of their online protests and their principled way of protesting, eventually they also abandoned their disruptive tactics, having been intimidated by the intensifying restrictions and punitiveness of the UK cybercrime/cyberterrorist regime.[75]

Politicised web-artists (artivists) have also resorted to activities with illegal and politically expressive effects, such as distributing viruses with a political message or hacking into websites and modifying digital artworks. These artists use their technological interventions to protest various political and economic phenomena, from the ‘commodification’ of artistic expression and the intensification of intellectual property restrictions to the neo-liberal, capitalist policies, adopted by governments or the environmental indifference of corporations.[76]

One such group had been EpidemiC, which had focused primarily, but not exclusively on viruses, seeking to uncover the artistic and communicative potential in viral code.[77] The code of the virus they created with 0100101110101101.org, another artivist group, was written as a story trying to communicate the positive aspects of viruses and their undue demonisation. Its code was circulated at a web-art festival through various online and offline means, and was even given to anti-virus companies as a show of the artists’ benign intentions.[78] EpidemiC also created, amongst other projects, a free Windows-based

[73] DJNZ and The Action Tool Development Group of the Electrohippies Collective, 'Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?' (2001) 34 Leonardo 269.

[74] ibid 273.

[75] The Electrohippies Collective (n 56).

[76] Vegh (n 59) 77; see also Lani Boyd, 'The Yes Men and Activism in the Information Age' (MA Thesis, Louisiana State University and Agricultural and Mechanical College 2005).

[77] For their general projects see ibid 193-5.

[78] See Mathias Klang, 'A Critical Look at the Regulation of Computer Viruses' (2003) 11 International Journal of Law and Information Technology 162, 177-8.

program, called ‘Anti-Mafia Action Sharing’, which utilised file-sharing software to help coordinate virtual sit-ins.[79]

0100101110101101.org is another similarly oriented pair of artists and their activities have included many legally ambiguous actions, such as artistic viruses and modifications of online artworks. For example, in the late 90s they created fake websites similar to those offered to limited subscribers-buyers by online galleries and even mutated the works on display, which resulted in legal action by the duplicated virtual galleries’ owners.[80] The purpose was to instigate discussion on intellectual property rights and unveil the pretences of originality and uniqueness in digital works that could be perfectly and easily reproduced digitally.[81] In another potentially illegal intervention, they hacked the website of a web art festival, randomly mixing the exhibits with the artists’ names.[82] Despite the lack of any legal consequences for the two artists, their performance led to the dismissal of the curator and the banning of the conference causing the pair to abandon such controversial performances in the future.[83]

The above groups break cybercriminal laws in order to facilitate the communication of their political messages and performances. However, they also develop software like Floodnet or AntiMafia, which could be considered violations of cybercriminal laws directly or inchoately, as can be used to facilitate, computer modification and impairment.[84] A group that is involved solely in the development of such tools is Hacktivismo, an offshoot of the hacker group Cult of the Dead Cow (cDc).[85] Hacktivismo focuses on promoting freedom of information and the privacy of citizens online. They develop software for bypassing

[79] EpidemiC, 'Antimafia: The Action Sharing' (*EpidemiC,* 2002) <http://epidemic.ws/antimafia/action.php?lng=en> accessed 20 September 2011.

[80] 0100101110101101.org, 'Copies' (*0100101110101101.org,* 1999-2000) <http://www.0100101110101101.org/home/copies/index.html> accessed 20 September 2011

[81] Nathan Castle, 'Internet Art and Radicalsim in the Digital Culture Industry' (2000) <http://www.lulu.com/items/volume_1/89000/89324/2/preview/netart_preview.pdf> accessed 16 June 2011 27-8; 0100101110101101.org, 'Copies' (n 80).

[82] 0100101110101101.Org, 'The K Thing: Story of an Infamous Online Performance' (*0100101110101101.org,* 2001) <http://www.0100101110101101.org/home> accessed 20 September 2011.

[83] ibid; Tatiana Bazzichelli, *Networking: The Net as Artwork* (*Digital Aesthetics Research Center*, Aarhus University, Aarhus 2008) 200-1.

[84] Ch 4, Part 3.3.2 The further criminalisation of inchoate offences.

[85] Samuel (n 59) 183; Hacktivismo, 'About Hacktivismo' (*Hacktivismo,* undated) <http://www.hacktivismo.com/about/index.php> accessed 20 September 2011.

censorship filters or safeguarding sensitive data from surveillance and security breaches through encryption and security scanning tools. Naturally, in an era where political conflicts in information networks focus on expression and privacy, their actions have a political hue.[86] Hacktivismo also have strict principles in relation to their chosen tactics, arguing that in democratic regimes the employment of protest methods, such as virtual sit-ins, defacements and viruses, essentially prevent expression or distort information, thus failing to promote free speech.[87] This issue will be extensively discussed in the next chapter.

Regarding their projects, even before the explicit formation of Hacktivismo, cDc circulated politically oriented software, such as 'Back Orifice', which took advantage of security weaknesses in Windows to facilitate the distant controlling of the compromised computer or network. The goal was to inform users about security flaws in Windows Operating System (OS) and pressure Microsoft to patch the holes 'Back Orifice' could exploit.[88] Such a tool, though, could inevitably be employed to realise the same effect that it was created to prevent and it was exactly this presumption that cDc wanted to take advantage of, in order to induce Microsoft to patch the flaw urgently and avoid risking user security.

Apart from other encryption tools, which appear less controversial, but could still facilitate the distribution of illegal material, such as child pornography,[89] their latest controversial work is 'Goolag Scanner'. This application utilises the Google search engine to uncover website vulnerabilities. Naturally, its dual nature as a security-enhancing application or a tool that enables hackers to find back-doors to websites has rendered it

[86] Oxblood Ruffin, 'Hacktivism: From Here to There' (*cDc Communications,* 06 March 2004) <http://www.cultdeadcow.com/cDc_files/cDc-0384.html> accessed 20 September 2011.

[87] Gar Warner 'Internet Anarchy: Anonymous Crowds Flex Their Muscles' (*CyberCrime and Doing Time*, 13 December 2010) <http://garwarner.blogspot.com/2010/12/internet-anarchy-anonymous-crowds-flex.html> accessed 13 August 2011.

[88] Tim Jordan, *Activism!: Direct Action, Hacktivism and the Future of Society* (Reaktion Books, London 2002) 130-1.

[89] Other projects include 'Torpark', an anonymising web browser that can even be used with a memory stick, hindering the traceability of user identities and 'Shatterchat', which is an encryption-imbued instant message relaying system. Tim Jordan, *Hacking: Digital Media and Technological Determinism* (Polity, Cambridge 2008) 74-75; Mib, 'cDc Releases Goolag Scanner '(*Hacktivismo,* 20 February 2008) <http://www.hacktivismo.com/news/> accessed 20 September 2011; Hacktivismo have also developed Camera/Shy, another encryption application, enabling the hiding of messages in media images. Jordan and Taylor (n 46) 109-110.

controversial.[90] Hacktivismo tools were released under Hacktivismo's Enhanced-Source Software License Agreement (HESSLA), imposing an obligation of legal, democratic use of the software they release in an attempt to prevent malevolent uses.[91] However, the impossibility of monitoring the use of Hacktivismo's tools, which are freely available renders the applicability of the license's terms reliant on the goodwill of the users, without any concrete assurance that these tools will not facilitate cybercriminal actions.

2.2.2 Anonymous and the second era of hacktivism

The groups discussed in the previous section characterise the initial phase of hacktivism. However, contemporarily, the most prolific and popular hacktivist collective is that of 'Anonymous'. Anonymous is essentially an identity that can be adopted by anyone, rather than an actual group, lacking memberships and encompassing many factions with potentially different ideological and tactical orientations, but often common goals.[92] Nevertheless, the more common tactics of Anonymous involve symbolic tactics, such as defacements and virtual sit-ins and therefore it could be said that parts, at least, of Anonymous, continue the tradition of ECD,[93] despite some activities also undertaken under the banner of Anonymous, such as theft and publication of information, which are less expressive and more morally controversial.

Anonymous originates from 4chan,[94] a collection of diverse message boards, ranging from Japanese anime to sports and music downloading. 4chan initially aimed to promote interaction between similarly interested people and eventually the organising of online

[90] Mike Barbwise, 'Google Scanning - Is It Legal?.' (*H-Online.com,* 20 February 2008) <http://www.h-online.com/security/features/Google-scanning-is-it-legal-746155.html> accessed 29 October 2010.

[91] Samuel, (n 59) 95-6; HESSLA explicitly prohibits the introduction of spy-ware, surveillance technology, or other undesirable code into HESSLA-licensed programs and any use of the software by any government that has any policy or practice of violating human rights. The license decentralises enforcement power, empowering plain end-users to act as enforcers. Ruffin, 'Hacktivism: From Here to There' (n 86).

[92] Luke Allnutt 'Old-School Hacker Oxblood Ruffin Discusses Anonymous and the Future of *Hacktivism' (Tangled Web,* 08 June 2011) <http://www.rferl.org/content/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html> accessed 20 September 2011.

[93] Anonymous 'Fragmented Plurality: An Interview with Gabriella Coleman' (*The Breaking Time*, 14 April 2011) <http://thebreakingtime.typepad.com/the_breaking_time/2011/04/an-enormous-plurality-an-interview-with-gabriella-coleman.html> accessed 20 May 2011.

[94] See 4chan website: http://www.4chan.org/ accessed 25 June 2012.

pranks for the lulz (slang for laughs). The sense of community and exchange of ideas that was cultured in 4chan discussion boards and collective projects led to the development of a pre-political character for many participants and even attracted more politicised ones.[95] As it has been argued, '[...] part of Anonymous has over the last three years moved from disaggregated practices rooted in the culture of trolling[96] to also become a rhizomatic and collective form of action catalysed and moved forward by a series of world events and political interventions.'[97]

This politicisation has even created a rift in 4chan, with lulz-oriented members (hatefags) expressing their disapproval of this transmutation from a fun-based collective to a socio-political entity.[98] On the other side, some more radical members of the politicised factions have also deemed that the activities organised were not adequately confrontational. The diversity of views has also led to the birth of splinter groups, such as the Anonymous Anarchist Action and LulzSec, which distanced themselves from the ethical dictates elaborated by many members of Anonymous, which focus on primarily expressive ECD.[99] However, these groups have not been very active, with Lulzsec members even being arrested after a hacking spree of 50 days.[100] Such fragmentations demonstrate clearly the lack of unanimity in Anonymous, which is crucial in understanding that, despite the

[95] Anonymous (n 93).

[96] As it is described in Wikipedia: 'a troll is someone who posts inflammatory, extraneous, or off-topic messages in an online community, such as an online discussion forum, chat room, or blog, with the primary intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion.' Wikipedia, 'Troll (Internet)' <http://en.wikipedia.org/wiki/Troll_(Internet)> accessed 05/11/2011.

[97] Gabriella E. Coleman, 'Anonymous: From the Lulz to Collective Action' (*The New Everyday,* 06 April 2011) <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action> accessed 21 September 2011.

[98] Adrian Crenshaw, 'Crude, Inconsistent Threat: Understanding Anonymous' (*Irongeek,* 2011) <http://www.irongeek.com/i.php?page=security/understanding-anonymous> accessed 21 September 2011.

[99] Harrison Myers, 'Anonymous Anarchist Action Hacktivist Group Founded' (*libcom.org,* 10 March 2011) <http://libcom.org/news/anonymous-anarchist-action-hacktivist-group-founded-10032011> accessed 22 September 2011; Charles Arthur, 'Lulzsec: what they did, who they were and how they were caught' (The *Guardian,* 16 May 2013). <http://www.guardian.co.uk/technology/2013/may/16/lulzsec-hacking-fbi-jail> accessed 20 June 2013.

[100] Susan Watts, 'Former Lulzsec Hacker Jake Davis on His Motivations' (*BBC,* 16 May 2013) <http://www.bbc.co.uk/news/technology-22526021> accessed 18 May 2013.

controversy surrounding the name of the collective, there are factions that behave within the limits of online political morality and promote beneficial activities.[101]

Anonymous functions in a directly democratic way as decision-making is based on voting by those participating in the iRC channels.[102] In Anonymous, only a few participants are deemed to be actual hackers, while many participants are computer 'geeks' - users interested in the content of the group - as well as more politically minded individuals and activists.[103] There is no concrete organising core or a spokesperson or leader, but the iRC channels are operated by more experienced members, which have increasing influence in decisions and are also burdened with imparting and employing the channels' constantly evolving self-regulatory norms, such as avoiding the targeting of media or the incitement of violence.[104]

Despite the democratic nature of such a structure, it has also been argued that making sense of the erratic discussions in the chaotic iRC can be a daunting task that could hinder democratic participation, rather than reinforce it.[105] Moreover, the lack of known representatives/organisers is also one of the weaknesses of the group, since its representation is done anonymously and from random groups or individuals that might be using the Anonymous identity in order to serve their own purposes, such as de-legitimisation or personal gratification.[106] Furthermore, Anonymous have often adopted confrontational and retaliatory rhetoric, potentially due to the collective's anti-authoritarian origins and the excitement of its numerous young participants, which can, however, obscure their moral intentions due to its aggressive style, which can often signal damaging and retaliatory, rather than expressive intentions.[107] Although pseudonymity and anonymity was a norm in the 4chan fora, hence the name of the collective, it has also been

[101] Anonymous, 'Anonymous Is Not Unanimous' (*Pastebin,* 17 August 2011) <http://pastebin.com/4vprKdXH> accessed 20 December 2011.

[102] Coleman (n 97).

[103] Anonymous (n 93).

[104] Coleman (n 97).

[105] Stephen Mansfield-Devine, 'Anonymous: Serious Threat or Mere Annoyance?' (2011) 1 Network Security 4, 7.

[106] Kevin Rawlinson, 'Inside Anonymous: The "Hacktivists" in Their Own Words' (*Independent*, 2011) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/inside-anonymous-the-quothacktivistsquot-in-their-own-words-2294935.html> accessed 21 September 2011.

[107] Anonymous have named their Wikileaks operation Operation Payback and their main punch-line is 'we do not forgive, we do not forget.' Also similar language can be seen in iRC chat discussions, when decisions on protests are being realised. See Warner (n 87).

advocated as a needed precaution against criminal prosecutions and personal attacks.[108] For the same reason of avoiding undue state surveillance, anonymity is even suggested during real-life protests organised by the group, where many protesters affiliating themselves with the collective wear Guy Fawkes masks, using the facade of the iconic revolutionary as their official 'trademark'.[109]

However, although the leaderless, memberless collective can be perceived as a disorganised, uncontrollable mob, assessments of Anonymous' operations suggest that the collective can indeed behave with an, albeit loose, political conscience and organisation in the form of a 'diffuse crowd'.[110] As it is argued, Anonymous often comes together because of the citizens' need to do something about common socio-political concerns, without a clear understanding of how to realise their goals, yet behaving in a more rational, conscientious manner, where the members have the option to participate or not, without being overwhelmed by a mob mentality.[111] They also say that their goal is not disruption and disturbance per se, but to create symbolic effects and raise awareness with their activities.[112]

Anonymous employ many diverse and often controversial tactics, ranging from virtual sit-ins and defacements of websites to more controversial acts, such as information theft and exposure of classified information.[113] Anonymous have also developed their own software for facilitating virtual sit-ins, called Low Orbit Ion Cannon (LOIC). The software can be connected to general command centre, the Hivemind of the collective, so that it automatically acknowledges the targets decided upon and engages in the protest when the designated time is reached.[114] The LOIC software does not include anonymisation software and cannot be used easily with such software, which means that users can eventually be

[108] See comments from alleged Anonymous in Scot Terban, 'Anonymous and Their Alleged Propagandist Barrett Brown' (*Infosec Island,* 10 March 2011) <https://www.infosecisland.com/blogview/12441-Anonymous-and-Their-Alleged-Propagandist-Barrett-Brown.html> accessed 28 September 2011.

[109] Coleman (n 97).

[110] Warner (n 87).

[111] ibid.

[112] Liam Fox, 'From Hacktivists to Spammers: Is Anonymous Failing?' (*News Junkie Post,* 12 December 2010) <http://newsjunkiepost.com/2010/12/12/from-hacktivists-to-spammers-is-anonymous-failing/> accessed 28 September 2011.

[113] For the various tactics employed see: Crenshaw (n 98).

[114] Elinor Mills, 'Wikileaks Fans Should Think before They Botnet' (*CNet News,* 10 December 2010) <http://news.cnet.com/8301-27080_3-20025373-245.html> accessed 28 September 2011.

traced through their IP address, thus retaining a basic way of identification.[115] Having seen the serious legal consequences of the lack of anonymity, some Anons have discussed developing a more advanced, anonymising LOIC-style tool.[116]

Anonymous became very widely known for their virtual sit-ins in support of Wikileaks at the end of 2010, where thousands of users participated.[117] However, they have been active since 2006, with their targets and exploits becoming gradually more serious and politicised.[118] What first gained them publicity were their protests against certain censoring attempts from the Church of Scientology.[119] For these protests, two individuals have pled guilty to computer damage charges due to their participating in the protests, having faced at least one year imprisonment, probation, fines and restitution penalties.[120] More than 14 members of Anonymous are awaiting trial in US courts in relation to the Wikileaks supporting protests against Paypal, with charges for conspiracy and criminal damage to computers that could reach up to 15 years in prison.[121] At least four members have also been tried in the UK under similar charges of conspiracy to cause computer impairment, with a person, Weatherhead, who did not plead guilty, receiving 18 months in prison.[122]

[115] Ryan Singel 'Dutch Arrest Teen for Pro-Wikileaks Attack on Visa and Mastercard Websites' (*Threat Level,* 09 December 2010) <http://www.wired.com/threatlevel/2010/12/wikileaks_anonymous_arrests/#seealsoaff033736dd3e21e1f35daab3a12f8f9> accessed 12 August 2011.

[116] Jon Leyden, 'Anonymous Unsheathes New, Potent Attack Weapon' (*The Register*, 04 August 2011) <http://www.theregister.co.uk/2011/08/04/anon_develops_loic_ddos_alternative/> accessed 11 September 2011

[117] Coleman (n 97).

[118] Their activities started from harassing a virtual hotels and white supremacists in order to protest discriminatory behaviour and facilitating the apprehension of an online child predator. Trimegisto 'History of Anonymous Hacktivism' (*The Trembling Uterus Blog*, 26 January 2011) <http://tremblinguterus.blogspot.com/2011/01/history-of-anonymous-hacktivism.html> accessed 28 September 2011.

[119] Coleman (n 97).

[120] Anonymous 'Teenage Hacker Admits Scientology Cyber-Attack USA v. Guzner – Information' (*Secretdox,* 18 October 2008) <http://secretdox.wordpress.com/2008/10/18/usa-v-guzner-plea-agreement-for-defendant-dmitriy-guzner/> accessed 20 May 2011; See *US v Guzner* (New Jersey, Dist. Court) Case No. 2:09-cr-00087; David Kravets 'Guilty Plea in 'Anonymous' DDoS Scientology Attack' (*ThreatLevel,* 26 January 2010) <http://www.wired.com/threatlevel/2010/01/guilty-plea-in-scientology-ddos-attack/> accessed 20 May 2011.

[121] Howard Mintz, ''Anonymous' Defendants Appear in San Jose Federal Court in Paypal Cyberattack Case' (*Mercury News,* 01 September 2011) <http://sip-trunking.tmcnet.com/news/2011/09/01/5747845.htm> accessed 01 September 2011.

[122] *R v Weatherhead, Rhodes, Gibson, and Burchall*, (Unreported) Southwark Crown Court, 24 January 2013**;** Josh Halliday, 'Anonymous Hackers Jailed for Cyber Attacks' (*The Guardian,* 24 January 2013) <http://www.guardian.co.uk/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks> accessed 18 June 2013.

Many more alleged Anonymous protesters have been arrested or are investigated in various countries,[123] yet Anonymous have been active, taking part in struggles all over the world for online and offline issues. Having analysed hacktivism and its developments let us now discuss what the aims and the methodology of the following analysis and what each of the following chapters will include.

3. Aims and methodological considerations

All the hacktivist tactics discussed above entail some degree of intrusion and disruption, usually in the form of adding, modifying, extracting information and, consequently, damaging or hindering the full functionality of computer systems and networks. The basic provisions that apply to these activities entailing unauthorised access, obtaining of information or impairment are those relating to computer damage or impairment.[124] For example, in the US, there are various provisions in the updated Computer Fraud and Abuse Act (CFAA) of 1986 which could be applicable to the above 'hacktions'.[125] The UK analogy would be the Computer Misuse Act of 1990 (CMA).[126] The thesis will attempt to highlight how the focus on these cybercime laws and a hierarchical 'command and control' approach

[123] Mary Watkins, Tim Bradshaw, and Joseph Menn, 'Global Police Moves against 'Hacktivists'' (*The Financial Times,* 27 January 2011) <http://www.ft.com/cms/s/0/db6f5ab0-2a34-11e0-b906-00144feab49a.html#axzz1YaNDtzCj> accessed 21 September 2011; Giles Tremlett and Agencies In Istanbul, 'Turkish Arrests Intensify Global War between Hacker Activists and Police' (*The Guardian*, 13 June 2011) <http://www.guardian.co.uk/technology/2011/jun/13/turkish-arrests-global-war-hackers-police> accessed 21 September 2011; John Leyden, 'Spanish Poice Cuff Three Anonymous Hack Suspects' (*The Register,* 10 June 2011) <http://www.theregister.co.uk/2011/06/10/spain_anonymous_arrests/> accessed 21 September 2011.

[124] The Honourable Marshall Jarrett et al.,'Prosecuting Computer Crimes' (Criminal Division Computer Crime and Intellectual Property Section Criminal Division, Department of Justice, Office of Legal Education Executive Office for United States Attorneys, Washington D.C.) <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf> accessed 20 May 2011, 44.

[125] 18 U.S.C., Part I, Title 47, Section 1030 (Fraud and related activity in connection with computers) Here the commonly used name of the provision as the Computer Fraud and Abuse Act 1986 (CFAA) will be used; The CFAA contains provisions relating to unauthorised obtaining of information Section 1030(a)(2), unauthorised access to federal computers Section 1030(a)(3) and intentional, reckless or negligent damage provisions that are directly applicable to most of these actions Section 1030(a)(5) For detailed analysis see Ch 4, Part 3.2 The applicable unauthorised access offences and 3.3 The dominating provision of computer damage.

[126] (c.18) The CMA 1990 contains provisions relating to unauthorised access (Section 1) and impairment (Section 3) and criminalisation of hacking tools (Section 3A), which would be directly applicable to these hacktivist tactics. See Ch 4, Part 3.2 The applicable unauthorised access offences and 3.3 The dominating provision of computer damage.

for dealing with hacktivism might be an inappropriate regulatory tool for dealing with hacktivism in efficient and just ways. The thesis will, then, attempt to find potentially better solutions by broadening the scope of the regulatory actors and tools embracing, thus, the new theoretical trends of networked regulation and applying them to shaping a better regulatory environment for hacktivism.

In terms of methodological approach, the thesis will extend beyond a pure black-letter law, doctrinal approach, to adopt a socio-legal one. The complexity of the phenomenon of hacktivism and of regulating cyberspace per se as a new, global and technologically-created space would suggest, if not require, that assessments and conclusions be based on more than primary legal sources and commentary on these sources. Following the current trends that dictate a broader and more inclusive approach to regulatory discussion, the thesis will also entail analyses of wider conceptions of regulation that engage with more actors and methods than a hierarchical, law-based, 'command and control' approach.[127] Consequently, apart from primary source analysis, which will be a crucial part of the discussion, the thesis will also engage with relevant aspects of other theoretical areas, such as criminology, political and communications theories and regulation theories.

As seen above,[128] the main regulatory conflict in the area of hacktivism is between exercising civil liberties, such as organising and protesting online, as they have been generally established in liberal, western democracies, on the one hand, and the radicalisation of cybercriminal law and cybersecurity regulations, on the other hand. Consequently, the framework that will be adopted for the analysis will be that of the values of contemporary western democratic regimes, which are becoming increasingly structured on value-conflicts between civil liberties on the one hand and public safety and order on the other, and have established protections for citizen rights that are in constant interplay with criminal justice processes and security policies, such as those inspiring and criminalising hacktivism. Furthermore, western democratic regimes have more actively persecuted hacktivist actions and are, therefore, the ideal legal and political framework for the analysis.

Finally, one more challenge will have to be addressed: choosing the specific jurisdictions, from these western liberal democracies from which the thesis will draw more specific

[127] Part 1.1 Defining regulation.
[128] Part 1.3 Information and power in the networks.

examples and arguments. If one were to assess all of them, the large number of liberal democratic regimes with many differences in criminal law, civil liberties and socio-political background would make the analysis impossibly long and diverse. Moreover, this thesis does not aim to be an exercise in comparative research, but to identify central problems in the treatment of hacktivism in jurisdictions that these issues are gradually being considered more important as these jurisdictions experience substantial hacktivist activity. Therefore, the main sources, such as legislation and case-law examples, but also additional socio-political elements will be sourced from specific jurisdictions that appear most appropriate for developing a discussion on hacktivism and regulation. An ideal forum for the discussion of this thesis will be the United States and secondarily the United Kingdom for various important reasons.

First, the terrorist attacks in the US and the UK have increased socio-political and legislative attention to politically-motivated deviancy; a trend that has generated wider discussion and regulatory activity around phenomena that might entail elements of political contestation and security, such as hacktivism.[129] An additional reason for using the above jurisdictions is the importance of both these cybercriminal regimes, which have the longest history and have been a great influence internationally.[130] Both the US and the UK also fit the general political framework chosen for the thesis, being organised on liberal democratic bases. They also demonstrate a long history of dealing both philosophically and legally with controversial political activities, such as illegal symbolic protests and, thus, have developed respective amounts of relevant litigation and commentary. Furthermore, these regimes are indicative of how criminal and cybercriminal law systems have gradually incorporated the current socio-political and economic trends of security and risk control in the liberal western world and in a rights-based political system. Naturally, these factors and tensions are not all unique to these jurisdictions, nor are they equally intense in both of them, but it appears that both the US and UK have shown the most activity and intensity in responding to hacktivism, which renders them the most appropriate examples for structuring a comprehensive critical analysis. Nonetheless, where appropriate, examples from other jurisdictions will be discussed in order to demonstrate the generalised nature of a particular argument discussed or show that certain tendencies might be characteristic of the Anglo-

[129] Marcus J. Ranum, *The Myth of Homeland Security* (Wiley Publishing Inc, Indiana 2004) 12.

[130] The 1984 Counterfeit Access Device and Computer Fraud and Abuse Act constituted the first legislative attempt to deal with computer crime internationally.

Saxon axis and more moderate in other jurisdictions. The reduced focus on other jurisdictions also flows from the almost total lack of examples in relation to hacktivist prosecutions in jurisdictions beyond the US and the UK[131]. Therefore, the above choice of the Anglo-Saxon axis is not so much a matter of convenience, but also an inevitable consequence of the recently increased impact of hacktivist actions in those two countries and the consequent limited number of cases and examples that exist beyond these countries.

4. Chapter breakdown

The analysis is separated in chapters that are interrelated. The current chapter has set the scene regarding the Internet as a new space for contesting powers, has defined the dominant elements in relation to the existing power conflicts and has highlighted the role of hacktivism as an innovative political practice and a manifestation of counterpower on informational networks. Afterwards, it defined hacktivism, as it will be examined in the rest of the thesis and gave us an initial idea of what the problems in regulating hacktivism might be and the direction that will be followed for remedying any potential problems.

Apart from demonstrating the intrinsic role of hacktivism in the central debates of cyberspace, the second aim is to assess the potential justifiability and legitimacy of these activities by demonstrating their potential for being realised based on certain moral standards. Chapter Two will, thus, focus more specifically on hacktivism as a potentially moral and non-harmful political activity, in order to concretise the qualities of hacktivism that differentiate it from plain criminal law-breaking and legitimise it politically. This analysis will further reinforce the arguments that support the merits, and the consequent need for paying special regulatory attention towards hacktivism as an activity that is more than simple security compromises, but can also be a politically legitimate, moral and useful way of expressing dissent online. For this process, the chapter will extract criteria of moral justifiability from the theory of civil disobedience. It will further discuss whether and to what extent such criteria would be applicable today for assessing the justifiability of an online illegal political practice, how these criteria might be reinterpreted and rationalised

[131] For the UK, the case-law examples are only from England and therefore a focus on the English legal system will be inevitable.

on contemporary socio-political realities, and whether hacktivism can satisfy these elements as a philosophy and practice.

The next aim will be to discuss the level and nature of punishment that would be justifiable according to criminal justice theories for activities that entail the characteristics that have been established in the previous two chapters for hacktivism. This process will be realised in Chapter Three and will lead to the identification of criteria in relation to the appropriate extent and nature of punishment for hacktivism, based on criteria of efficiency and justice in relation to imposing criminal punishment. The analysis in this chapter will clarify the justness and efficiency of the various types and levels of punishment, when applied to hacktivism. The conclusions and arguments drawn in this chapter will contribute to the shaping of criteria for assessing the appropriateness of the current laws and policies that impact on the regulation of hacktivism, based on considerations of justice and human rights, such as privacy, freedom of expression and proportionality, but also of facilitating cybersecurity and preventing criminal excesses.

Chapter Four will assess the current conditions that impact on the regulation of hacktivism and the currently preferred ways for dealing with these activities. This assessment will focus on the consistency and adequacy of contemporary regulatory forces impacting on hacktivism with the expectations of appropriateness established in relation to regulating hacktivism. These criteria established in the previous chapters will mainly relate to the fair and just treatment of hacktivists, the respect of their rights as well as the efficient prevention of dangerous protests and the maintenance of functionality of networks and security of users in cyberspace. Essentially, this discussion will try to identify any flaws in the current regime in promoting the goals mentioned above, by analysing not only the law per se, but other engaged regulating factors, such as private online companies, the public, the media and hacktivists themselves. The goal is to evaluate whether the focus on law and mainly the cybercriminal justice system can respond efficiently and justly to such political phenomena.

The ultimate step, which will constitute Chapter Five, will be to find ways for the treatment of hacktivism, as an online illegal, yet potentially legitimate, political practice in a democratic society, based on the values and regulatory expectations discussed in the preceding chapters, mainly justice and efficiency. Criteria for steering the analysis towards certain directions will also, however, flow, apart from the nature of hacktivism, from more general considerations relating to regulating conflicts of rights and security online and the need to promote more efficient and just solutions in securing cyberspace, while enabling users to exercise their rights. This chapter will, thus, examine how existing modes of regulation could be improved and will also suggest additional solutions in forming a network of mutually reinforcing propositions.

The thesis will close with a short chapter discussing the conclusions drawn from the whole analysis and expressing the author's views and hopes for the future of hacktivism within the cybersecurity framework and the role he sees for academics in this effort. This work aims to provide useful thoughts and arguments beyond just the phenomenon of hacktivism. It further relates to the management of serious information conflicts in cyberspace, the future of civil liberties in cyberspace, the general trends in regulating cybersecurity, and the shaping and interplay of different actors in the online regulatory structure in which hacktivism is a regulating and regulated part. The examination of the hacktivism paradigm, thus, also opens new paths and contributes to discussions of cyberspace security and rights regulation through acknowledging the importance of hacktivism for online politics and its role in the shaping of the cyberspace.

CHAPTER 2

ASSESSING THE MORAL JUSTIFIABILITY OF HACKTIVISM

The introduction has provided us with the broad socio-political and legal framework in which hacktivism takes place, has familiarised us with the specifics of hacktivist groups, aims and tactics and has set the problems and the goals of this analysis. More particularly, Chapter One has demonstrated the prima facie illegality of hacktivism, but also its important role in online power conflicts as part of manifestation of resistance movements against information control trends and a series of tactics that supplement physical protests against social injustices and policies of information control. The next question that is of interest to this thesis is whether hacktivism is different to criminal law-breaking and whether the fulfilling of certain moral standards could actually justify the practice and establish the need for different treatment to plain criminality. Hacktivists often argue, for example, that their acts are akin to free expression or acts of civil disobedience (CD) and emphasise the ethical qualities and tactical analogies between hacktivism and free expression or CD that render their activities legitimate political protest.[1] This view has been contested, though, as the controversial nature of hacktivists' online tactics, which are generally considered prima facie criminal,[2] has led people to question the morality and potential usefulness of such activities.[3]

This chapter will, therefore, attempt to assess the existence of the moral dimension to hacktivist practices that could be argued to differentiate them from plain criminal law-breaking. The first step will be to assess the link between freedom of expression and hacktivism, and to demonstrate the potential differentiating factors which mainly focus on the law-breaking element of hacktivism. Subsequently, in order to demonstrate the moral justifiability of hacktivism, despite its illegality, I will distil certain criteria of moral

[1] Ricardo Dominguez, 'Electronic Disobedience Post-9/11' (2008) 22 Third Text 661*;*
DJNZ and The Action Tool Development Group of the Electrohippies Collective, 'Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?' (2001) 34 Leonardo 269.

[2] See Ch 1, Part 3. Aims and methodological considerations.

[3] Alexandra W. Samuel, 'Hacktivism and the Future of Political Participation' (DPhil Thesis, Harvard University 2004) 101, 141, 210; Andrew Calabrese, 'Virtual Nonviolence? Civil Disobedience and Political Violence in the Information Age' (2004) 6 info <www.emeraldinsight.com/1463-6697.htm> accessed 15 June 2010.

justifiability from theories of CD, to which hacktivism relates as a philosophy and practice. Another reason for choosing CD theory in order to extract criteria for assessing the morality of illegal political protests is the extensive literature analysing the moral dimensions of CD and the implications of its justifiability.

However, trying to assess new forms of resistance, such as hacktivism, based on criteria shaped during a pre-Internet era, when most of CD theory was developed, could end up generating inapplicable or distorted analogies. Although this analysis will attempt to demonstrate that perceptions and assessments of moral legitimacy could and should be perceived based on well-established principles that operate within the existing framework of western democracies, the new social, economic and political conditions introduced or exacerbated by the introduction of digital technologies should not be disregarded. The updating of moral and political arguments is required for providing a realistic and not just an abstract, theoretical moral analysis. This process acknowledges that with societies' gradual progress, moral and political perceptions cannot remain unchanged, since that would render them obsolete or stifle social progress.

Consequently, the first step in assessing the justifiability of hacktivism is to discuss why it is not justified under the political right of free expression. The following section will highlight the similarities, but also the crucial differences, between hacktivism and protected free expression that eliminate the chances of hacktivism being capable of being totally identified with protected free speech and, thus, avoiding criminal sanctions for the exercise of that right.

1. Free expression and hacktivism

Hacktivists have tried to analogise their actions to free expression, portraying their conduct as inherently expressive and similar to actual speech.[4] Symbolic political acts, such as those employed by hacktivists and more traditional, offline CD protesters, is usually some form of conduct that takes its expressive dimension according to the context it takes place in, thus,

[4] John W. Whitehead, 'Civil Disobedience and Operation Rescue: A Historical and Theoretical Analysis' (1991) 48 Washington & Lee Law Review 77, 103; Barbara J. Katz, 'Civil Disobedience and the First Amendment' (1985) 32 UCLA Law Review 904, 906; Dominguez, 'Electronic Disobedience Post-9/11' (n 1).

acquiring a certain meaning without being explicitly put in words. For example, a sit-in at a University Dean's office by students for reasons relating to unequal University policies, is, thus, upgraded from a mere illegal act of trespass to a message about the students' disapproval of the protested policies. Although expression through symbolic conduct that can also entail law-breaking is often more implicit than pure verbal expression of dissent, symbolic protests are usually part of a wider campaign for a political cause, where the role of such acts is to intensify the expression of dissent through direct speech. It is also often a fact that the illegality of expressive conduct relates to an act of disruption (such as trespass, breach of peace or computer impairment for hacktivists) in order to attract additional attention.

That element of disruption and the usual illegality of symbolic speech acts are, however, crucial differentiating factors between fully protected pure speech and conduct-facilitated expression, despite views that argue that 'actions which are clearly symbolic and only incidentally illegal ought to be protected for what they are.'[5] In the US, where free speech jurisprudence is far more extensive and detailed, the right to free expression (free speech) and the consequent protection is afforded to pure speech, which has been considered distinct to expression through symbolic acts.[6] The common law origin of a right to protest is that people could do whatever they wanted, so long as their actions did not break the law.[7] Therefore, under common law, illegal acts of expression would not be considered protectable legal speech. Even pure speech in the form of verbal (slander) or written expression (libel) can be exempt from free speech protection and, thus, punishable.[8] Moreover, even when exercising freedom of expression in the forms of speech, assembly or petition, one is not allowed to commit a breach of the peace,[9] while restrictions can be

[5] Robert Hall, 'Legal Toleration of Civil Disobedience' (1971) 81 Ethics 128*,* 132. Mead equates peaceful speech with symbolic and incidentally or inevitably obstructive/disruptive protests with the requirement that protests do not entail disproportionate disruption that could seriously impair the functionality of the protesters' targets. He considers such activities to be legitimate civic responses that should be considered lawful, unless there is contradicting evidence. David Mead, *The New Law of Peaceful Protest: Rights and Regulation in the Human Rights Act Era* (Hart Publishing, Oxford 2010) 11-2.

[6] Katz (n 4) 906-7.

[7] Mead (n 5) 26; Noah Hampson, 'Hacktivism: A New Breed of Protest in a Networked World' (2012) 35 Boston College International & Comparative Law Review 511, 526-7.

[8] Susan Tiefenbrun, 'Civil Disobedience and the US Constitution' (2003) 32 Southwestern University Law Review 677*,* 697. Criminal libel was only abolished for England, Wales and Northern Ireland in 2010 with the Coroners and Justice Act of 2009, Ch 3, section 73.

[9] J. L. Legrande, 'Nonviolent Civil Disobedience and Police Enforcement Policy' (1967) 58 The Journal of Criminal Law, Criminology, and Police Science 393, 395-6.

imposed in relation to the time, space and manner of the expression of dissent.[10] After all, free expression is not absolute and can be restricted by conflicting serious interests, such as the protection of private property or public safety.[11] Even in the US, where the First Amendment is considered fundamental, case-law has prioritised property rights and has accepted time, manner and place restrictions, if these restrictions do not relate to the content of the speech, are narrowly tailored, serve a governmental goal and allow for speech alternatives.[12] Hacktivism, being an outright violation of cybercrime laws of unauthorised access and/or impairment also impacts on property rights of others, be they state or private entities, and thus would definitely not qualify as protected expression.

Case-law in both the US and UK, has given priority to private property rights, when conflicting with free expression, even for pure speech-related events on spaces that are not designated for public speaking, despite these places simulating public fora, such as shopping malls. The US case of *Lloyd v Tanner*[13] demonstrates how the denial to leave the mall's premises at the request of the owner, when leafleting against the war in Vietnam, was considered a violation of the mall owners' right of private property. The court concluded that the cause of the protest was unrelated to the place of protest (the mall), as there were also adequate alternative places for expression that were publicly accessible, such as pavements, adjacent to the shopping mall. A similar conclusion was reached by the court in *Appleby v UK*.[14] In *Appleby*, the rights of property of the mall-owning company Postel were considered superior to the right of free expression (art.10 ECHR) and assembly (art.11 ECHR) of three protesters that were petitioning inside a mall against the decision of the council to build on the sole remaining public playing field. A similar approach was followed in the UK case of *City of London v Samede & Ors.* [15] Here, protesters were prevented from protesting within the privately-owned Canary Wharf area, even though the

[10] Hampson (n 7) 527. Mead (n 5) 100.

[11] Council of Europe, 'The European Convention on Human Rights' (Rome, 1950) art 10.2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. See case-law for the US free speech right, which usually offers far wider protection but gives in to violations of private property rights.

[12] *Ward v Rock Against Racism* 491 U.S. 781 (1989).

[13] *Lloyd* Corp. *v Tanner* 407 U.S. 551 (1972) (*Tanner*).

[14] (2003) 37 EHRR 38 (*Appleby*).

[15] *City of London v Samede & Ors* [2012] EWHC 34 QB (*Samede*).

cause of their protest, the economic crisis facilitated by the banks hosted in Canary Wharf, was very relevant to the space the protesters had chosen for the protests.[16]

The above cases demonstrate that, in order for the protest to be allowed, there has to be a direct link between the cause protested and the private space, where the speech-act is realised and there also has to be a lack of alternative spaces for protesting that are relatively close to the place chosen for the protest. For example in the US case of *Amalgamated Food Employees Union Local 590 v Logan Valley Plaza, Inc*[17] the picketing against a company operating within a shopping mall was considered protected speech. The two crucial elements justifying this decision were, first, that the protest was strictly related to the space where it was taking place and, secondly, there were no public space alternatives close by due to the nature of the area where the shopping mall was located. However, *Tanner* has been the dominant precedent in the US having superseded *Logan Valley*, whereas *Appleby* is also considered an authority in the EU.

A rationale similar to *Tanner* and *Samede* seems to be followed in cyberspace cases regarding pure speech and private property. For example, the court in *CyberPromotions* found that, if non-Internet alternatives exist that would allow expression to reach the desired public, then private actors, such as America Online, could not be forced to accept speech on their private online networks in order for speech to reach its subscribers.[18] The existence of legitimate alternatives online, such as websites, social networking sites and blogs allow for speech even on the same medium and therefore hacktivists would not be justified in arguing a lack of chances to express their protest online. Moreover, the tendency to give priority to private property rather than speech online discussed above, has been further reinforced by designating even public-access computers as non-public spaces

[16] ibid.

[17] 391 U.S. 308 (1968) (*Logan Valley*).

[18] In *Cyber Promotions, Inc. v America Online, Inc*, 948 F. Supp. 436 (E.D. Pa. 1996) (*CyberPromotions*). The court assessed whether AOL, by providing Internet access and email service to its subscribers could be considered a public forum, therefore, obliging AOL to abstain from imposing any speech restrictions on its services, much like the state was obliged to abstain from restricting speech in designated public forums, such as town squares or public parks. After applying a test to assess whether AOL was providing a state traditionally provided by the state or whether an elaborate financial or regulatory nexus or symbiotic relationship existed between AOL and the state, the court argued that AOL's service did not have the character of a public forum and, thus, was under no obligation to allow speech as a private space. See Dawn C. Nunziato, 'The Death of the Public Forum in Cyberspace,' (2005) 20 Berkeley Technology Law Journal 1115, 1136.

in the case of *US v American Library Association*.[19] In this case, the US Supreme court argued that public library Internet access did not constitute a public forum and, therefore, filtering restrictions on patrons' access to information were considered constitutional.

A question arising from the above cases is whether the intrinsic lack of adjacent, or any, public spaces, such as roads pavements or town squares in cyberspace could have an impact on the decision to allow speech on private websites. Perhaps one could argue that, much like *Logan Valley* above,[20] the lack of any interstitial spaces online in conjunction with the potential relevance of the protest to the website accessed could justify the act of unauthorised access of hacktivists. Consequently, if protesters wish to express their dissent at a space adjacent to the agent that is the cause of their protest, breaking cybercrime laws by accessing and impairing or modifying webpages without authorisation becomes inevitable. However, the disruptive effect of the designated function of the website that hacktivist tactics usually cause will negate any claim to legality. This is further reinforced by the decision of the *Tanner* court which argued that protectable speech should have no disruptive effect to the proper function of the protested space, for the space itself and its visitors.[21] It appears then from the analysis of this subsection that it is unrealistic to argue that hacktivism is identical to free expression and, consequently, fully protected from liability, at least under the current legal status quo. This is even more so since courts in the US have considered even the advice and suggestion to commit virtual sit-ins as unprotected speech,[22] while numerous arrests and criminal convictions of cyberprotesters in the US and the UK clearly show the general presumption is to consider hacktivism criminal, rather than an exercise of free speech.[23]

The sole exception can perhaps be found in Germany, where the court, trying a case of virtual sit-ins against Lufthansa's website for its assistance to state deportation policies, found that a lack of any substantial coercion of the online protesting impairment would

[19] In 539 U.S. 194 (2003)(*Library Association*) the US Supreme court argued that public library Internet access did not constitute a public forum and, therefore, filtering restrictions on patrons' access to information were considered constitutional.

[20] See (n 17).

[21] The court respected the private property right and the desire of the owners of the mall to prevent protests that could cause disruption or annoy any of the patrons.

[22] *US v Fullmer* 584 F.3d 132 (3d Cir. 2009) (*Fullmer*).

[23] See Ch 4, Part 3. The impact of cybercrime laws on hacktivism.

allow it to be equated to protected speech.[24] The German appellate court exonerated these protesters, after the court of first instance had found them guilty and had imposed a monetary fine, and the exoneration spread optimism as to the future legality of virtual sit-ins.[25] However, prosecution was based on charges of coercion rather than cybercrime law and the trials took place before the explicit EU-wide criminalisation of denial of service attacks;[26] two elements that render the following of the Lufthansa precedent highly unlikely, even in Germany, since cybercrime provisions will most likely be used for virtual sit-ins currently.[27] Nevertheless, this case demonstrates the acknowledgment of the expressive quality inherent in hacktivism, which constitutes part of hacktivism's justifiability, even if not adequately strong to prove exonerating for the law-breaking hacktivist practices. The analysis will now move to discuss the links and analogies between CD and hacktivism, and the basis and criteria for justifying illegal political practices.

2. The links between CD and hacktivism

2.1 Definitions and initial clarifications

Rawls describes CD as 'a public, nonviolent, conscientious yet political act, contrary to law usually done with the aim of bringing about a change in the law or policies of the government.'[28] For Habermas, it is a 'non-violent, symbolic, and illegal form of protest, undertaken with the intention of appealing to the formal institutions of the state on the one hand and the sense of justice of the wider political community on the other'.[29] Power is even more inclusive: 'it is a deliberate, public, articulated infraction of regime rules, aimed

[24] See the Lufthansa virtual sit-in case: *OberlandesGericht Frankfurt am Main v Thomas Vogel* (No. 1 Ss 319/05) case available in German: <http://www.libertad.de/service/downloads/pdf/olg220506.pdf>
See also commentary in English in European Digital Rights, 'Frankfurt Appellate Court says Online Demonstration Is Not Coercion' (*European Digital Rights,* 07 June 2006) <http://www.edri.org/edrigram/number4.11/demonstration> accessed 20 May 2011.

[25] Dominguez, 'Electronic Disobedience Post-9/11' (n 1).

[26] For denial of service and hacktivist use of such tactics see 2.2.1 The first era of hacktivism and the birth of electronic civil disobedience.

[27] Federico Biancuzzi, 'Achtung! New German Laws on Cybercrime' (*Security Focus,* 10 July 2007) <http://www.securityfocus.com/columnists/448> accessed 20 May 2011.

[28] John Rawls, *The Theory of Justice* (Harvard University Press, Cambridge 1999) 320.

[29] Juergen Habermas, 'Civil Disobedience: Litmus Test for the Democratic Constitutional State' (1985) 30 Berkeley Journal of Sociology 95, 99.

at changing a regime's law or policy, non-injurious to the physical person, considerate of the rights of others, and pursued within the state's jurisdiction to expand and apply the democratic ethos.'[30] The definition of hacktivism as: 'the fusion of methods of systems modification or reconfiguration that transgress cybercrime laws and target computer systems and networks to produce or simulate effects that confer a political message or protest a particular policy'[31] is indicative of, at least, an initial connection between CD and hacktivism.

The aspect of 'civil', of course, is the one entailing the qualities that render the disobedience in CD morally justifiable and will be discussed extensively in the rest of the chapter. For now let us briefly discuss the more practical aspect of law-breaking. The primary core element that defines CD is the voluntary violation of a valid law of the state with public repercussions. Two types of political disobedience/law-breaking have been identified. One form involves directly violating a law, which is considered unjust in order to induce a reconsideration of the law or achieve a constitutional review (direct CD). The other category relates to staging a protest through breaking other valid laws, usually property, or in the case of hacktivists, cybercrime laws, as a means to communicate a political message, attract attention to an injustice, sensitise public opinion and induce the regime to consider a change of policy (indirect CD).[32] Usually the focus of hacktivist practices is on criticising other political decisions and social injustices and not on protesting against cybercrime laws per se, therefore, their protests are mainly indirect, using the legal violations as a means for creating a political message in online spaces that are relevant to their various causes.[33] In fact the violation of cybercrime laws could be an inevitable requirement for realising their expressive protests, as seen in the previous section on free expression.[34] Therefore, the main tactics examined here (virtual sit-ins, virus distributions and web-defacements/redirects) should be considered similar to indirect CD. Regarding data thefts,

[30] Paul F. Power, 'Civil Disobedience as Functional Opposition' (1972) 34 The Journal of Politics 37, 40.

[31] For definitions see Samuel (n 3) 1-2.

[32] Hugo A. Bedau, 'Civil Disobedience in Focus: Introduction' in Hugo A. Bedau (ed), *Civil Disobedience in Focus* (Routledge, London 2002) 50.

[33] An exception could be the creation of a virus that attempts to express concerns about the undue demonisation of viral software in contemporary cybercrime regimes. 0100101110101101.org, 'Contagious Paranoia: 0100101110101101.org Spreads a New Computer Virus' (0100101110101101.org, 2011) <http://www.0100101110101101.org/home/biennale_py/index.html> accessed 26 December 2011.

[34] Part 2.1. Free expression and hacktivism.

the symbolic element being secondary in them, or in some cases absent, which as will be seen in this chapter makes the analogising of data thefts to symbolic, indirect CD, both practically and in terms of moral justifiability, challenging, since these acts constitute a more radical form of hacktivism that borders on direct action[35]. Irrespective of data thefts, hacktivist actions are generally oriented towards publicising an injustice, communicating public disaffection to the authorities and educating the public through their symbolic simulations.[36]

The rest of the chapter will deal with the various elements that the concept 'civil' entails. Initially, the analysis will focus on theories of justice and their ways of potentially justifying moral law-breaking. As will be seen, the levels of moral justification of disobedience to law range from prohibitive to very accepting, depending on the theoretical lens one employs. Inevitably, the analysis of the various theories of justice below will not aim to show that disobedience is generally accepted, but will aim instead to highlight the contestable nature of the justification of political law-breaking and to identify the elements that play a crucial role in shaping the decisions for the justifiability of disobedience. Because hacktivism relates to indirect disobedience, a focus will be given to this aspect, yet this discussion will be placed in a more general account of disobedience that will eventually lead us to the specific arguments of indirect CD.

2.2 The moral justifiability of CD and hacktivism

2.2.1 Natural law

Natural law theories acknowledge the existence of a divine or natural moral order that is eternal and universal, with principles that are superior to man-made laws.[37] We can see this conflict dating back to the years of ancient Greek tragedies. The Sophoclean tragedy

[35] CAE characterises direct action as policy subversion tactics, including information thefts and more destructive interventions that have a more coercive and less expressive character than ECD, which is mainly based on creating a public spectacle. Critical Art Ensemble, *Digital Resistance* (Autonomedia, New York 2001) 14.

[36] Hacktivism is not realised as direct violation of a law deemed unjust in order to force an examination of a law's constitutionality in courts, nor is it a case of conscientious objection, which relates to a denial to act as obliged by a specific law (passive law-breaking) and so these two kinds of disobedience will not be analysed here any further.

[37] Howard Davies and David Holdcroft, *Jurisprudence: Text and Commentary* (Butterworths & Co Ltd, London 1991) 149.

Antigone' presents a moral dilemma of obedience to man-made or divine laws, demonstrating the conflicting duties of Antigone, on the one hand, to follow the divine edict of burying her dead brother and on the other hand, abiding by her uncle and King's command that he is left unburied.[38]

For natural theorists, most man-made laws are presumed to be informed by those higher principles, integrating them into the legal system, which, thus, establishes its morality and legitimacy. Obedience to law is, therefore, a moral duty arising from the presumed alignment of positive laws with natural, moral laws, which essentially results in harmonious and peaceful living. For example, the Catholic Christian tradition supported obedience to law based on equating political authority to God's word and considering rulers' decisions as divine edicts not to be challenged.[39]

Nevertheless, natural law theorists accept the prospect of disobedience to a law, if that law is unjust in the sense of conflicting with the natural law principles. St. Thomas Aquinas, for one, considers positive laws that have failed to uphold natural principles to be violent acts rather than law and, consequently, invalid and undeserving of citizens' obedience, since obedience flows from the laws' agreement with higher natural principles.[40] Even for immoral, man-made laws, though, Aquinas inserts a qualification to disobedience, suggesting that, if disobedience could create a corrupting example (scandal) or serious social disturbance, it should be avoided.[41]

An approach similar to Aquinas has been adopted by Finnis, who also differentiates between positive and natural law. In his book, 'Natural Law and Natural Rights', Finnis identifies seven 'intrinsic goods' the respect of which he relates to moral living: life, knowledge, play, aesthetic experience, sociability (friendship), practical reasonableness and religion.[42] For Finnis, the move from seeking to achieve those goods to actually making moral choices is realised through a series of principles that are 'the basic requirements of practical reasonableness', such as avoiding compromises to basic goods regardless of the benefit, refraining from arbitrary discrimination among persons and basic goods and

[38] Mark Griffith, *Sophocles: Antigone* (Cambridge University Press, Cambridge 1999).

[39] ibid 210-1.

[40] Brian Bix, *Jurisprudence: Theory and Context* (5th edn, Thomson Reuters (Legal) Limited, London 2009) 70.

[41] Ian McLeod, *Legal Theory* (2nd edn, Palgrave MacMillan, New York 2003) 53-4.

[42] John Finnis, *Natural Law and Natural Rights* (Oxford University Press, Oxford 2011).

promoting the communal good.[43] Finnis considers law as a way of realising or obtaining some goods within a social system shaped by interactions with other people and that is why law should be consistent with the above requirements of ethical reasonableness.[44] He does not deny unjust laws their legitimacy, but like Aquinas argues that they lack the moral authority that commands obedience, although compliance with immoral laws can still be morally advisable, if it is necessary for upholding just institutions.[45] This qualification reflects Finnis' fear that morally justifying disobedience of important, yet unjust, laws could eventually lead to a general disregard of the legal system.[46]

Finnis and Aquinas advocate direct disobedience of seriously unjust laws, especially if the law-breaking would not generate undue harm to important rights and social goods. Although both accept the morality of disobeying unjust positive laws, they link the acceptance of disobedience, even of unjust laws, to a consideration of future consequences of the disobedient act for society. Moral justification of indirect CD would be much more challenging, since there is not an issue of moral invalidity of the law being disobeyed. Especially since Finnis rejects any utilitarian argument for disobedience,[47] it would be contestableto argue that indirect disobedience, when ultimately promoting natural law, would be considered justifiable. The only rationale that could perhaps be considered as justifying indirect disobedience is to argue that the indirect law-breaking is a legitimate defence to the act of violence that the invalid law represents, along the lines suggested by Aquinas. As will be seen later in the thesis,[48]similar defences regarding the necessity of disobedience in order for an injustice to be avoided or the violation of a law in order to promote a higher law incorporating higher moral standards have been posed by protesters and have been seriously considered by courts.

Adopting a more procedural approach to natural law, Fuller articulates certain procedural standards, the lacking of which indicates the moral deficiency of laws. According to Fuller then, the lack of set rules, a failure to publish the law, retroactive legislation, failure to make laws understandable, promulgation of contradictive rules or rules that pose

[43] Bix (n 40) 76-7.
[44] ibid 77.
[45] McLeod (n 41) 118-9.
[46] ibid; Davies and Holdcroft (n 37) 199.
[47] Bix (n 40) 76.
[48] Ch 4, Part 5.2.3 The role of the jury.

requirements beyond the subjects' powers, frequent changes in rules and failure of congruence between the letter of the law and its application are flaws that render laws immoral.[49] For Fuller, the maintenance of the inner moral standards of law can often be superior to the actual moral duty to obey, since a legal system contradicting these principles will often be immoral in itself.[50] Laws that contravene the above safeguards are considered immoral and, therefore, unworthy of obedience. Fuller acknowledges that in the cases of regimes employing a series of illegitimate laws, it would be up to the individual citizen to decide whether to obey even the legitimate rules of such a regime or not, as the regime will be lacking legitimacy per se.[51]

Fuller does not appear to be as sensitive as Aquinas and Finnis to the future consequences of disobedience and relates disobedience of laws, valid and invalid, to the general legitimacy that a regime acquires from its laws and the processes it employs to create them. For generally legitimate regimes though, such as those examined in the thesis, it would be extreme to argue that Fuller would justify disobedience of valid laws. It would appear, therefore, that natural law theorists, although very accepting of direct disobedience based on the alleged immorality of a law, would be reluctant to accept the moral justification of violating legitimate laws. There are, however, various theories that have more specifically discussed the justification of indirect CD.

2.2.2 Social contract theories: From Hobbes to Habermas and Rawls

The core premise of social contract theories is that citizens have conceded their natural rights to a sovereign power by forming a contract where they agree to obey the sovereign's commands in return for the maintenance of social peace and protection of their rights.[52] Hobbes argues that obedience should be maintained even in cases where the government is taking oppressive measures, because even that government will be better than no

[49] Lon Fuller, *The Morality of Law* (Revised edn, Yale University Press, New Haven 1969).

[50] Viewed more abstractly what Fuller concedes to, is that behaviour that is consistent with higher moral standards can often defeat the presumed moral directive that law should be maintained. Fuller's view is extreme rendering in most cases the legal system invalid if it does not meet his procedural criteria. See: ibid 39.

[51] ibid 40-1.

[52] Hobbes is a characteristic theorist of this primary contract-based rationale. Thomas Hobbes, *Leviathan* (1651) <http://oregonstate.edu/instruct/phl302/texts/hobbes/leviathan-contents.html> 20 June 2013.

government.[53] However, he argues that the duty to obey lasts up to the point where the sovereign appears impotent to protect the rights of citizens anymore.[54] However, Hobbes' theory focuses on disobedience as a solution to the impotence of the sovereign to fulfil the contract, rather than a tool that is employed mostly as a protest/correctional mechanism in democratic states of today.

Democracy-focused contract theories establish the obligation to obey based on a hypothetical pact between citizens and a government democratically elected by the people with a similar contract rationale, where citizens make concessions on their rights in order for their elected governmental representatives to provide rules that will guarantee social peace and protection of citizens' natural rights and impose sanctions for legal violations.[55] A duty of obedience on behalf of the citizens is, thus, founded on this implicit or promissory consent in exchange for protection of their rights and social peace, while other theories base obedience to state laws on the active participation of citizens in the democratic institutions and the receipt of the respective benefits the democratic legal order guarantees.[56]

This obligation to obey, though, is only maintained under the qualification that the state protects democratic institutions and acts within its powers and for the interest of the public, which it represents.[57] Within a democratic contract-based society, any consistently undemocratic or unjustifiable iniquitous treatment of citizens by the state would exceed the contractual terms and be unjust, since the extent of the state's authority is, arguably, as broad as the rights conceded to it and cannot act in authoritarian or arbitrary ways.[58] Consequently, if the state does not respect the citizens' moral rights and expectations, they can reassert their conceded rights in order to rebel and establish another contractual relationship with another sovereign that will not violate the obligation of ensuring social

[53] ibid, Ch 14.

[54] ibid.

[55] See John Locke, *Two Treatises of Government*, Book II, Second Treatise, para. 7-8 in Ian Shapiro (ed), *Two Treatises of Government and a Letter Concerning Toleration* (Yale University Press, London 2003) 102-3, 105, 109, 137-8.

[56] Greenawalt, *Conflicts of Law and Morality* (Oxford University Press, New York 1989) 63, M.B.E. Smith, 'Is There a Prima Facie Obligation to Obey the Law?' (1973) 82 The Yale Law Journal 950, 961-4.

[57] Greenawalt (n 56) 63-4.

[58] Jean-Jacques Rousseau, *The Social Contract* (The Penguin Group, London 2004) 32-6; McLeod (n 41) 58.

welfare.[59] Going beyond Hobbes, who only accepts disobedience in case of the sovereign's impotence to fulfil his function to preserve the peace, Locke, for example, accepts disobedience towards a government the practices of which excessively disrespect the rights the citizens have conceded to it.[60]

These contract theories seem to accept disobedience only as a solution for reinstating a new contract with a new sovereign and not as a correctional mechanism within the context of the existing government. These absolutist perceptions between full obedience and all-out disobedience in case of an oppressive government would fail to provide justification for disobedient tactics that operate without aspiring to an all-out rebellion, yet disobey valid laws in order to indicate to the citizens and the government that certain rights and liberties are excessively violated and that the situation should be remedied. If however, an all out disobedience is justifiable in cases of bad governance, could we consider indirect CD as a morally justifiable attempt to preserve the democratic social contract by highlighting existing problems in order to remedy these and prevent more generalised conditions of disobedience and unrest? Habermas and Rawls seem to focus more on the case of indirect CD and provide some answers.

Habermas enriches contract theories by introducing free and rational personal assessment of laws as a criterion for their legitimacy and a prerequisite for obedience in addition to the standard basis of coercion found in Hobbes.[61] Smith identifies two criteria for Habermas' conception of illegitimate law: violating basic rights of citizens and disregarding proper democratic deliberation in law-making.[62] The first element is straightforward and very similar to natural law theorisations. The second refers to cases where less influential minorities, politically and/or financially, are excluded from democratic deliberation processes or where powerful economic and political minorities promote decisions without engaging in public dialogue or manipulate decision-making with

[59] McLeod, (n 41) 58; Hannah Arendt, *Crises of the Republic* (4th edn, Harvest Books, San Diego 1972) 93.

[60] Alexander M. Bickel, 'Civil Disobedience and the Duty to Obey' (1973) 8 Gonzaga Law Review 199, 209; McLeod, (n 41) 58.

[61] Juergen Habermas and Martha Calhoun, 'Right and Violence: A German Trauma' (1985) 1 Cultural Critique 125, 134-5.

[62] William Smith, 'Civil Disobedience and Social Power: Reflections on Habermas' (2008) 7 Contemporary Political Theory 72, 79-80.

their influence.[63] Habermas acknowledges the potential obsolescence or corruption of democratic institutions by strong influences and he considers the democratic contract an open process, where its norms have to be consistently challenged and revised.[64]The challenging is realised through the generation of crises within the public sphere that reinvigorate the polity and ameliorate the inevitable communication and power deficits in contemporary democracies.[65]

Habermas submits that CD functions as a means for the polity to maintain its legitimacy by attempting to reinstate the moral balance implicit in the basic contractual arrangements that have been corrupted and by further developing these contractual terms, like an informal, crisis-inducing correctional device.[66] Consequently, indirect CD as a symbolic act of protest is considered justified as a means to reinstate the moral bases of deficient democratic regimes. The correctional function relates to the protests appealing to the core foundations of legitimacy of the constitutional democratic order, democratic deliberative decision-making and the protection of established citizen rights.[67] Essentially CD can reinstate marginalised citizens as participants in law development processes, from the formal procedures of which they might feel excluded, such as deliberation procedures, to facilitating the more direct exposure and confrontation of corruptive influences and deficiencies that could nullify the democratic social contract.[68] Consequently, for Habermas and Calhoun, CD is usually 'suspended between legitimacy and legality' and even though the state has a right to bring its perpetrators to justice, if it considers it necessary, it should do so with the consideration that such protesters are also guardians of the state's legitimacy.[69] In order to maintain the moral legitimacy of CD, Habermas articulates certain moral criteria that CD protesters will have to consider. These are the need for protesters to act publicly, non-violently and accept their punishment for their law-breaking, but also the

[63] ibid 81-2; See how the Supreme Court connected the elimination of limitations to spending money and effort in promoting or defeating political adversaries with free speech, surrendering election decisions even more to the influence of rich corporate elites. Adam Cohen, 'Case Study: The Supreme Court and Corporate Free Speech' *(Time,* 07 July 2010) <http://www.time.com/time/nation/article/0,8599,2001844,00.html> accessed 21 December 2012.

[64] Juergen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (William Rehg tr, Polity, Cambridge 1996) 384.

[65] ibid 382; Smith (n 62) 78.

[66] Habermas and Calhoun (n 61) 137.

[67] Smith (n 62) 79-80.

[68] ibid 78.

[69] Habermas and Calhoun (n 61) 137.

need to demonstrate respect for the legal order and justify their protest based on constitutional principles.[70]

Habermas' view engages with modern notions of CD and blends them with contract theories, thus providing us with a rationale for their moral justification. The challenging, deliberative and crisis-inducing basis for justifying CD, also relates to hacktivist tactics. After all, the hacktivists' main aim is to confront power on the informational level and provide alternative means for communicating dissent with the hope of sensitising the public and inducing influential and powerful groups to reconsider problematic policies and political decisions that bypass equal deliberative processes and violate citizens' rights.

Contract theories have developed further to focus on a fair play agreement between all citizens that requires obedience to function rather than an obligation to obey as a result of some commitment to a sovereign. Rawls builds his moral theory of justice on notions of fairness between co-citizens and he extensively discusses the moral justification of CD. Justice for Rawls is interrelated with fairness and equality. First, fairness, for Rawls, entails that duties and obligations derive from ethical principles, defined as principles people would have chosen, if their social status and interests were 'unknown' to them; his famous 'veil of ignorance'.[71] Secondly, Rawls also submits that societies are just, when they maintain conditions of equal opportunity between citizens within social institutions and that social and economic inequalities (i.e. of wealth, authority) are considered just, only if they result in compensating benefits for everyone, particularly the underprivileged.[72] For Rawls, the prima facie duty to obey the law and promote just institutions gives way only when disobedience is realised for the political reason of addressing the sense of justice in the community and for cases, where there is substantial and clear injustice.[73] Rawls designates as substantial injustices any serious infringements of the principles of equal liberty or fair equality of opportunity.[74] However, he also recognises that in contemporary pluralistic societies, absolute descriptions of justice would be void, as there is an abundance of liberal conceptions, which might share similar structural characteristics of society, yet

[70] ibid.

[71] John Rawls, *The Theory of Justice* (n 28) 301; John Rawls, 'Justice as Fairness: Political Not Metaphysical' (1985) 14 Philosophy and Public Affairs 223*,* 236-7.

[72] Rawls, *The Theory of Justice* (n 28) 13; Rawls, 'Justice as Fairness' 227-8;

[73] Rawls, *The Theory of Justice* (n 28) 326-7.

[74] ibid.

interpret and balance them differently.[75] This acknowledgment of the different perceptions of justice along with his acceptance of reasons for justifying disobedience, if it is opposing serious injustices, renders the moral justification of disobedience open to interpretation, thus, broadening its scope.

Rawls explicitly accepts the justifiability of CD and also discusses indirect CD. He acknowledges that sometimes, it is less harmful and practically feasible to break a minor law, such as trespass, in order to protest a major law that might be practically difficult to break, such as more abstract foreign policy decisions, or might have very grave consequences if directly violated for the purposes of protesting it, such as homicide.[76] Moreover, he acknowledges that protests might also relate to inaction of the government to take measures to prevent an ongoing injustice, where there is no law to be protested, but the object of the protest might be the creation of a law in order to deal with the injustice in question.[77] Rawls also argues that CD should not be confined to cases of constitutional challenge, since, if a law is considered unjust, the protesters will disobey it, even if it is eventually considered constitutional.[78] As he argues, 'CD expresses disobedience to law within the limits of fidelity to law, although it is at the outer edge thereof'.[79]

Rawls further discusses criteria he considers constitutive of CD as a morally justifiable practice. First, he believes that CD should be based on shared political principles of justice and not personal morality, religious beliefs or self-interest.[80] Rawls further focuses on the non-violent character of CD and argues that protesters should avoid harming other citizens or seriously impacting on their civil liberties, although he concedes that sometimes after legitimate, non-violent attempts have failed, force might be an acceptable option.[81] Another criterion influencing justifiability is whether CD is employed after an effort has been made to facilitate change through legitimate means. [82] However, Rawls accepts again, much like with the non-violence criterion, that if legitimate measures seem inefficient or

[75] John Rawls, *The Law of the Peoples; with the Idea of Public Reason Revisited* (Harvard University Press, London 2000) 14-5; Rawls, *The Theory of Justice* (n 28) 342.
[76] Rawls, *The Theory of Justice* (n 28) 320.
[77] Alan M. Schwarz, 'Civil Disobedience' (1970) 16 McGill Law Journal 542, 564.
[78] Rawls, *The Theory of Justice* (n 28) 320-1.
[79] ibid 322.
[80] ibid 321.
[81] ibid 322.
[82] ibid 327-8.

inaccessible in the particular context, the expectation of prior employment of legitimate means of change might not feature in the moral evaluation of CD.[83] Rawls also argues for coordination of CD between minorities with valid claims to exercise it in order for it not to become so pervasive as to severely weaken the rule of law, which he believes can be achieved through competent leadership.[84] Furthermore, he links the moral justifiability of CD to its potential punishment, arguing that the civil and moral nature of the act and its justifiability on the basis of political constitutional principles should lead the courts to either reduce the penalties or even suspend any punishment.[85] Even though he considers these elements constitutive of CD as a moral practice, at the same time he accepts that they can be relative criteria in relation to the specific context of the protest.

Rawls perceptions, despite the various restrictions, such as coordinated actions of minorities that might appear too abstract and overtly optimistic for the scale of contemporary politics, are important for modern CD and hacktivism because many such protests are realised against governmental and international organisations' decisions or even policies, which might be legal, yet still remain unreasonably unfair, disregard marginalised groups and weak minorities or even intensify already existing inequalities.[86] Rawls' analysis is particularly helpful because it combines elements of natural law and contract theories and explicitly articulates criteria that are commonly discussed by many theorists, such as non-violence or acceptance of punishment, thus, facilitating the distillation of the criteria of justifiability that this thesis will discuss in the next section. Moreover, Rawls' acknowledgment of the multicultural conceptions of justice, and the concessions he makes to the criteria he designates in relation to the particular context, emphasise the need for interpretive openness towards alternative moral views, thus, broadening the potential of moral justifiability of many controversial political activities, such as hacktivism. This relativism will become even clearer, when this analysis proceeds to

[83] ibid.

[84] ibid 328-9.

[85] ibid 339.

[86] Examples are the denial of states to sign the Kyoto agreement, the International Monetary Fund Memoranda in various countries considered greatly unfair, to the point of being illegitimate. For rising inequalities in the crisis era see: Mohammed Abbas, 'Economic Crisis Could Widen Inequality - Report' (*Reuters,* 10 October 2010) <http://uk.reuters.com/article/idUKTRE6992CY20101010> accessed 24 October 2010, Global Research, 'U.S. Social Inequality Income Gap Hits Record High' (*Market Oracle*, 29 September 2010) <http://www.marketoracle.co.uk/Article23088.html> accessed 24 October 2010.

assess the criteria of justification, but before that a very crucial justifying theory in relation to obedience should be discussed.

2.2.3 Utilitarianism

The moral basis of utilitarianism is the maximisation of an ultimate social good and a just practice is whichever promotes overall happiness or social well-being. According to Bentham, 'Nature has placed mankind under the governance of two sovereign masters, pain and pleasure. It is for them alone to point out what we ought to do, as well as to determine what we shall do.'[87] There are two major branches of utilitarianism. According to the first branch, 'Act Utilitarianism', since the moral aim is the maximisation of utility, moral acts will be those with the best or equally good consequences for the general welfare from all the alternatives open to the actor. A prima facie obligation to obey the law here flows from the fact that the state is an actor that is presumed to be maximising utility through laws that direct social living and, as such, following the laws of the state is usually considered the more utilitarian option.[88] However, this theory would also allow for instances of disobedience, both direct and also indirect, as it does not preclude the possibility of the superior utility of disobeying the law in particular contexts, where obedience might have less positive results. In the cases of CD, for example, the immorality of minor law-breaking, such as trespass, which normally impacts negatively on public welfare, could be subsumed by the high moral value of attempting to eliminate a much greater non-utilitarian condition, such as protesting against a social injustice.[89] This rationale is, thus, based on the preference of the lesser evil, which has even been codified as a criminal justification defence (necessity) as will be discussed later in the thesis.[90]

The second branch, 'Rule Utilitarianism' inserts another level of assessment between the act and the actual assessment of its utility, proposing that regulation of one's actions should be founded on rules that, when followed, generally lead to the maximisation of

[87] Jeremy Bentham, 'Introduction to the Principles of Morals and Legislation' in Alan Ryan (ed), *John Stuart Mill and Jeremy Bentham: Utilitarianism and Other Essays* (Penguin Group, London 1824) 65.
[88] Smith 'Is There a Prima Facie Obligation to Obey the Law?' (n 56) 965.
[89] William T. Blackstone, 'Civil Disobedience: Is It Justified?' (1969) 3 Georgia Law Review 679, 696.
[90] Ch 4, Part 5.2.3 The role of the jury.

utility.[91] This theory promotes consistent behaviours and law-abidingness, since it avoids being reduced to a balancing of results in each particular occasion and can, thus, support the moral rightness of an obligation to obey, even in cases where disobedience might produce better results short-term.[92] However, even this theory leaves space for disobedience, if there are strong moral reasons of self-interest or a clash with other important moral rules.[93]

The acceptance of disobedience, even in 'Rule Utilitarianism' is clarified by Mill, who enriches the theory of utility by introducing certain rights that formulate a more complete concept of justice based on rules and principles that usually produce utilitarian results. Mill specifies those rights as personal liberty, property or any other thing which belongs to a person by law, moral rights, just deserts, the protection of expectations raised by promised obligations and impartiality in the appointment of rights, which is also related to equal treatment.[94] Utilitarianism, as Mill explains, is not a theory that disregards justice for utility, but one that acknowledges the diversity of interpretations of justice and the inevitability of conflicts between those different interpretations in culturally diverse societies and finds utilitarianism as the best resolution for conflicting justice claims.[95]He argues, however, that although the rights and expectations constituting justice are of paramount social utility, yet, sometimes, one might be allowed to break laws that support some of the less important ethical duties, which in general should be followed, in order to serve a higher moral duty.[96]

In justifying direct CD, the dominant utilitarian rationale would, thus, be that, if a law or policy is seriously unjust, it would compromise social welfare by being enforced. Consequently, direct disobedience towards an unjust law is by itself utilitarian, presuming there is not a less immoral, yet equally efficient way of achieving similarly utilitarian

[91] Nigel E. Simmonds, *Central Issues in Jurisprudence* (3rd edn, Sweet and Maxwell Ltd, London 2008) 35.
[92] Greenawalt, *Conflicts of Law and Morality* (n 56) 105-6.
[93] ibid 106.
[94] John Stuart Mill, *Utilitarianism* (Original Eddition 1879, The Floating Press, 2009) 78-83, 90.
[95] ibid 99-104.
[96] As Mill says, 'Justice is a name for certain moral requirements, which, regarded collectively, stand higher in the scale of social utility, and are therefore of more paramount obligation, than any others; though particular cases may occur in which some other social duty is so important, as to overrule any one of the general maxims of justice.' ibid 113.

results.[97] Justification of indirect CD is also based on the rationale of a balance of conflicting disutilitarian actions. CD is employed, even though prima facie considered immoral as law-breaking of a normally utilitarian, legitimate law. In essence, justification is, therefore, based on the balancing of evils between the low immorality inherent in the breaking of a valid law as a protest act and the important moral aim of trying to change a seriously disutilitarian law. Utilitarianism also provides the possibility for justification of CD to rely, not just on appeal to the majority's sense of justice, but also on the need to protest against potential harms that derive from misguided, yet formally legitimate, political decisions, where the effect might be of great social disutility.[98] Although this lack of reliance on justice principles has been deemed potentially problematic for the justification of disobedience,[99] Greenawalt asserts that protesting against foreseeably harmful policies could be morally justifiable, because one should not expect citizens to 'disregard their fears about harms that do not derive from injustice'.[100] After all, it appears that contemporarily, many offline CD and hacktivist protests are also realised for reasons relating to lack of social consideration in political decision-making.[101]

2.2.4 Conclusion

This section has reviewed various jurisprudential and political theories, with the aim of showing that, despite the general acceptance of a prima facie obligation of citizens to obey the law, disobedience has been considered morally acceptable, at least for most theories, when done for reasons that are based on strong moral grounds. Natural lawyers accept disobedience towards laws that are considered unjust, but would probably refrain from justifying disobedience against laws that are considered moral and, thus, legitimate. Social

[97] In some cases, illegal, indirect disobedience might be less disutilitarian and harmful than legal or direct CD For example: Direct disobedience towards an unjust homicide law would of course result in much greater disutility than an indirect, publicising protest. Kimberley Brownlee, 'The Communicative Aspects of Civil Disobedience and Lawful Punishment' (2006) 1 Criminal Law and Philosophy Journal 179, 183-4; Joseph Raz, *The Authority of Law: Essays on Law and Morality* (Oxford University Press, Oxford 1979) 269.

[98] As Greenawalt says*: '*If [...] what has happened is only a very bad policy decision and disobedience is likely to produce a careful reappraisal and possible reversal, the disobedience might well be warranted. The intensity of opposition demonstrated by self-sacrificing disobedience can serve to promote re-examination of crucial factual data as well as claims of justice*.'* Greenawalt, *Conflicts of Law and Morality* (n 56) 234-5.

[99] Daniel Markovits, 'Democratic Disobedience' (2005) 114 The Yale Law Journal 1897, 1900-1.

[100] Greenawalt, *Conflicts of Law and Morality* (n 56) 234.

[101] Markovits (n 99) 1901.

contract theories also appear reluctant to justify law-breaking, unless the social conditions have become so patently unjust that generalised disobedience against the regime would be morally acceptable in order for another, more functional contract to be instituted between the citizens and a more just sovereign. Both natural lawyers and contract theorists fear that moral acceptance of disobedience of laws, even if unjust, could cause a more general disregard for the rule of law by setting a bad example and trivialising disobedience to the point, where it might be taken up on a more general scale.

On the other hand, theorists, such as Habermas, Rawls, Mill and Greenawalt seem to accept that disobedience could be justified morally, if based on strong moral reasons, even if breaking legitimate laws. Habermas and Rawls even designate explicit moral criteria for CD.[102] These include non-violence, protesting openly and for a moral political purpose, the need to trust in the legal system and use of CD only after legitimate measures of amelioration have been attempted, the coordination of protesters to minimise disobedience, the realisation of the protest within the normative framework of the contemporary societies and acceptance of the general validity of the legal order and of the punishment society would hand down. Utilitarians also highlight the importance of proportionality for the justifiability of CD, arguing for efficiency and relevance (the protest should be the least or equally harmful means for achieving the utilitarian goal) and essentially a balancing of harms between the consequences of the disobedient act and the consequences of the injustice protested against, which also could translate to non-violence or using CD as a last resort, similarly to what Rawls suggests.

However, the main conclusion is that, even for criteria that have been deemed constitutive of CD, such as non-violence, the particular context of a protest plays a crucial role in assessing the extent they could be followed. Contextuality is, thus, the most crucial overarching element that informs most discussions of the moral justifiability of CD and any reviewing of the designated criteria influencing the moral justifiability of an act of political disobedience should not consider moral criteria as absolute edicts, but more as indications of the potential for justifiability. The use of the term justifiability, instead of justification declares exactly the graduated nature of the notion. This relativity of justifiability will

[102] See Part ***2.2.2 Social contract theories: From Hobbes to Habermas and Rawls***.

become more obvious in the following sections, where the moral criteria identified above will be discussed more extensively and will be linked to hacktivism. The relation of hacktivism to these criteria will also indicate the level of justifiability it could attain, although the importance of the justifiability criteria is strictly related to context, which could lead us to morally justify protests based on a different reading of these criteria in accordance to the current socio-political conditions and the nature of the protests.[103] Let us discuss these criteria and the relation of hacktivism to these in more detail.

3. The criteria of justifiability

3.1 Conscientious, yet political

3.1.1 Conscientious belief in an injustice

As CD is a response to a perceived injustice, a basic moral criterion is the conscientious belief of the protesters that there is a serious injustice justifying their protesting. The question arises as to whether a general public consensus is required in relation to the actual existence of an injustice or whether personal beliefs would suffice. The motivation for the illegal act has to involve a moral reason that deserves more respect than the law violated.[104] However, in contemporary societies, sanctifying personal conscience unqualifiedly has been considered dangerous, as it could lead to justifying activities that relate to every personal whim and render CD dangerous for the social order if exercised superficially.[105] Rawls tries to avoid this potential generalisation of justifying disobedience by underlining that CD should be based on established political principles of justice and not just personal morality, religious beliefs or self-interest.[106]That is why he describes CD as 'conscientious, yet political'. According to Rawls, for a person to act with autonomy and responsibility, she would have to find and assess how the political principles that inform the interpretation of the constitution relate to her particular context of disobedience and

[103] Blackstone (n 89) 681-2; Rawls, *The Theory of Justice* (n 28) 319;
Expectations of non-violence, for example, will have to be perceived in a less absolutist way, which is obvious by Power's definition that defines non-violence as non-injurious to persons, especially since defining violence in the strict sense in cyberspace is challenging. See 3.2 Non-violence.

[104] Bedau, 'Civil Disobedience in Focus: Introduction' (n 32) 9.

[105] Power (n 30) 42.

[106] Rawls, *The Theory of Justice* (n 28) 320-1.

decide her course of action in accordance to how she thinks these principles should be interpreted.[107] Only after the above process, could the decision to disobey, even if the interpretation is wrong, be deemed conscientious and, thus, moral, rather than just selfish.[108]After all, Rawls accepts that there cannot be a single correct interpretation of constitutional principles, even if coming from the legislature or the courts and, therefore, citizens are responsible for their interpretation of the principles of justice and their conduct according to these.[109] This primary criterion is also often related to hacktivist actions, since in most protests there is indeed a reference to the violation of certain important rights or important principles, from privacy and free speech to international agreements and well acknowledged social interests, such as ecology.[110]

The broader interpretation Rawls gives to conscientious protesting also relates to another important concern, namely, whether CD as an informal, law-breaking, policy-changing tool contradicts formal, majority-based decisions within a democratic regime. Considering CD by minorities as morally legitimate in a democracy could, arguably, compromise decisions taken by democratically elected legislatures and lead to the majority acceding to the coercive minorities' demands.[111] This raises a more general question of whether CD is in conflict with democracy if protests originate from minorities and/or aim to change the policies of the officially elected government by the majority. As discussed above, a crucial criterion of justification is the respect for the current legal order, which constitutes an overarching moral criterion that relates to many elements, from the one currently discussed to the criteria of submitting to punishment and employing legal, democratic measures of amelioration before resorting to illegal means, which will be discussed in the rest of this chapter. Do CD acts and hacktivism undermine majoritarian democracies by morally justifying actions that would oppose the decisions of the government, thus, injuring democracy?

In order to assess whether CD and hacktivism violate the democratic ethos through challenging majoritarian decisions based on minority interpretations of morality and justice,

[107] ibid 341.
[108] ibid.
[109] ibid 342.
[110] See Ch 1, Part 1.5 The role of hacktivists as hacker/political entities of counterpower.
[111] Steven R. Schlesinger, 'Civil Disobedience: The Problem of Selective Obedience to Law' (1976) 3 Hastings Constitutional Law Quarterly 947, 953; Rawls, *The Theory of Justice* (n 28) 312; Smith (n 62); Menachem M. Kellner, 'Democracy and Civil Disobedience' (1975) 37 The Journal of Politics 899, 900.

one should first assess the importance of majority rule for democratic regimes. Despite its importance for democratic decision-making, majority rule does not absolutely overrule all other concerns of a democratic society, especially since ensuring inclusive processes of deliberating decisions by the public and the protection of minorities' interests are also crucial democratic elements that balance majority rule.[112] Electoral systems can even be manipulated in ways that suit the stronger parties and further weaken the representation of minority interests.[113] In fact in many democratic states, electoral systems have led to coalition governments, due to a weakness of one party to get even the relevant majority in votes that is required for getting a parliament majority.[114] Therefore, majority rule cannot be considered flawless and protests that challenge injustices that the majority has facilitated against minorities should not be characterised undemocratic, since their purpose could often be to act correctively against majorities' excesses or corrupt decisions of the majority's representatives.[115] Moreover, since CD and hacktivism often involve appeals to the majority for facilitating change, this implies that the protesters have an ultimate belief in the majority's sensitisation and amelioration potential. It would thus be an oxymoron to criticise CD protesters as disregardful of the majority, either as government representatives or the political body, since protesters essentially aspire to both these political bodies for change though their protests. One could, even, counter-argue that CD protests reinforce the rule of the majority by ultimately recognising its authority to correct the mistakes of its representatives, and, thus, does not try to disempower the majority. On the contrary, protestors usually attempt to increase the engagement of states and citizens in an active, creative discussion. Consequently, moral assessments should focus on whether the hacktivist efforts have a moral background informing their efforts as appeals to the majority and/or its representatives in response to potential deficiencies of the democratic governance.

[112] Rawls, *The Theory of Justice* (n 28) 313; Kellner (n 111) 901; The European Court of Human Rights in *Gorzelik v Poland* (2005) 40 EHRR has argued that democracy identifies with the protection of minorities and the avoidance of abuses of majority's dominant position: Mead (n 5) 32.
[113] See Part 3.5 Last resort.
[114] The UK and Greece and even Belgium, where there has even been a weakness in forming a coalition government for months, all demonstrate how governments could essentially end up representing minority views, where smaller coalition forces would often be forced to make political concessions in relation to their pre-election promises in order for the government not to fall apart. The Liberal Democrats case in the UK and the Democratic Left in Greece are again typical examples of how weaker coalition parties subordinate their views to the strongest, yet still minority in the country, party in the governing coalition.
[115] Alexander M. Bickel, 'Civil Disobedience and the Duty to Obey' (1973) 8 Gonzaga Law Review 199, 210; Habermas and Calhoun (n 61) 137.

3.1.2 The choice of tactics and coinciding consciences

Another relevant contested issue is whether the moral motivation for the conscientious act can be proven by the number of people joining the protest. Particularly in relation to the choice of tactics for online protests, small group protests have been characterised as selfish, undemocratic actions of technical and political arrogance.[116] Especially in cases where the activities are perpetrated by single hacktivists or small groups, such as redirects/defacements or the promulgation of a political virus, the above consideration becomes even more important.

Mass participation tactics, such as virtual sit-ins, are considered more indicative of the public acceptability and, thus, closer to a conscientious view that aligns with the popular interpretations of justice and less reliant on personal moral views. The more participative nature of virtual sit-ins decentralises the blameworthiness of illegal protests: something which virtual sit-ins protesters have claimed emphasises their democratic legitimisation.[117] However, the above argument would not always be valid, since less disruptive tactics, even if perpetrated by fewer people, such as a web-defacements, could be more appealing to the public than a mass online sit-in that could take off a website for hours and cause serious service disruption.[118] Gandhi even considered individual or small group CD far safer and less prone to corruption than massive acts, without considering it less morally legitimate, as longs as disobedience was consistent with the same moral cause as mass actions.[119]

Especially with the alleged trend that has seen networks of involuntarily engaged computers (botnets) being employed in order to enhance the disruptive effect of virtual sit-ins, one could argue that solitary or small group acts could indeed prove equally, if not more, morally legitimate. Even in these cases of botnet-enhanced virtual sit-ins, though,

[116] Kenneth E. Himma, 'Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?' (2005) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=799545#> accessed 19 June 2013, 17.

[117] Samuel (n 3) 12.

[118] Small scale actions like web-defacements often cause less disruption and inconvenience than mass actions, like virtual sit-ins. see Meiring De Villiers, 'Distributed Denial of Service: Law, Technology & Policy' (2007) Paper 7, University of New South Wales Faculty of Law Research Series, 1, 25-6.

[119] Vinit Haksar, 'The Right to Civil Disobedience' (2003) 41 Osgoode Hall Law Journal 415; For example, small groups could be more politically and tactically considerate, than more expansive collectives, such as with Anonymous, where motivations and beliefs of participants could vary. See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism.

one could adopt Raz's argument that the disobedient should only be responsible for the morality of his own acts.[120] Therefore, the fact that someone might be acting immorally by joining the virtual sit-in and using a botnet to enhance its effects should not undermine the justifiability of the initial, principled protestors cause.[121]

Consequently, there does not appear to be a direct link between the assessment of the moral conscientious character of disobedience and the actual choice of tactics or numbers of participants. The choice of tactics might even be related to the particular context and, thus, the amount of engaged protesters can be a matter of practicality and efficiency, since many tactics off- and online require or allow only for smaller groups.[122] After all, both offline CD and hacktivist acts cannot practically engage every person that might be supportive, while CD's and hacktivism's illegal character can also be discouraging for the masses for fear of punishment. If collective conscience behind the protest has expressly been against certain tactics, considering them excessive or inconsistent with the purposes and the goals set, the activities of an individual could be considered personal and detached from shared perceptions of injustice, and, thus, selfish and less justifiable.[123]

3.2 Non-violence

Non-violence is a common requirement in discussions of the moral justifiability of CD.[124] A requirement to avoid violence relates to preserving the proportionality of harms between the protesting law-breaking and the injustice the protest relates to, since physical injury to citizens would usually adversely impact on the justifiability of protests because physical harm will often be frowned upon as a means of protest and can also undermine the expressive character of the protest. A demand for non-violence is also considered important for preventing CD from deteriorating into serious social disorder, where harm to individuals and property destruction – both characteristic of violent behaviour – could lead to similar acts of retaliation and generalised vigilantism, even online, through technological countermeasures. The requirement for non-violence, thus, reflects the need for the protest

[120] Raz (n 97) 269.

[121] ibid.

[122] Web defacements and redirects are examples of individual or small group efforts, while a sit-in at a small office could not accommodate all the protesters that a march for a similar cause would.

[123] For example, Anonymous might criticise attacking certain websites as irrelevant to a cause and yet few members might proceed with a protest, despite the general condemnation of the choice.

[124] *The Theory of Justice* (n 28) 320; Habermas and Calhoun (n 61) 127-8, 132; Arendt (n 59) 76-77; Blackstone (n 89) 680-1.

to minimise challenges the state's monopoly on the use of coercive physical force, but also, mainly, the need to act in ways that would minimise any chances for serious harm or damage to citizens or property.[125] The fear that the justification of disobedience, especially when violent, could lead to generalised lawlessness and social disorder has been a common concern,[126] yet it has never been historically proven and has been considered an exaggeration by supporters and critics.[127] In fact, the contextual, multi-faceted nature of CD often involves minor violence, the total condemnation and exclusion of which from CD would be an unrealistic and disempowering demand of protesters.[128] After all, CD has also been considered as a means for correction of anti-social and unjust political decisions and even as a less harmful outlet of social disaffection, instead of more radical opposition, due to its symbolic, non-violent nature.[129] Hacktivism could also, partially, operate as a release valve for social tensions, indicating where public disaffection might be focusing before it becomes so radical, as to deteriorate into violent citizen outbursts. But how would we define violence?

3.2.1 Defining violence

The threshold between violence and non-violence is hard to define and the term 'violence' has often become distorted, since virtually any unwelcome activity might be considered violent, if it causes inconvenience or offence.[130] DeForrest proposes defining it by using accepted legal descriptions in order to prevent vagueness and exclude forms the law has

[125] Rawls, *The Theory of Justice* (n 28) 321-2.

[126] Raz (n 97) 237; Kent Greenawalt, 'A Contextual Approach to Disobedience' (1970) 70 Columbia Law Review 48, 56-7.

[127] Martin C. Loesch, 'Motive Testimony and a Civil Disobedience Justification' (1990) 5 Notre Dame Journal of Law, Ethics & Public Policy 1069, 1112-3; Generalisation of CD is usually the fault of unjustly or inefficiently acting authorities and will not be a direct consequence of accepting CD as legitimate. Alan M. Schwarz, 'Civil Disobedience' (1970) 16 McGill Law Journal 542, 553-4; Arendt (n 59) 69-70, 74; Rawls, *The Theory of Justice* (n 28) 342.

[128] Raz (n 97) 267; Schwarz (n 127) 565-6; Anthony D. Woozley, 'Civil Disobedience and Punishment' (1976) 86 Ethics 323, 325; Greenawalt, *Conflicts of Law and Morality* (n 56) 245.

[129] Rawls, *The Theory of Justice* (n 28) 336; Craig P. Colby, 'Civil Disobedience: A Case for Separate Treatment' (1968) 14 Wayne Law Review 1165, 1167-8. Arendt recognises that many changes in the US legal system have happened because of the pressure CD has exerted on reformative political mechanisms and legislatures: Arendt (n 59) 80-82; Moreover, the government is forced by confronting such incidents to also witness the social disaffection for its practices, realise its shortcomings and try to minimise points of friction with citizens. Power (n 30) 47.

[130] Mark E. DeForrest, 'Civil Disobedience: Its Nature and Role in the American Legal Landscape' (1998) 33 Gonzaga Law Review 653*,* 657-8.

not strictly prohibited.[131] A legal definition of violent crime could prove enlightening. According to the United States Code, Title 18, Part I, Chapter I, S. 16 'crime of violence' means:

> (a) an offense that has as an element the use, attempted use, or threatened use of physical force against the person or property of another, or
>
> (b) any other offense that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense.[132]

In the UK, Public Order Act 1986,[133] Section 8, defines violence as:

> [A]ny violent conduct, so that-
>
> (a) except in the context of affray, it includes violent conduct towards property as well as violent conduct towards persons, and
>
> (b) it is not restricted to conduct causing or intended to cause injury or damage but includes any other violent conduct (for example, throwing at or towards a person a missile of a kind capable of causing injury which does not hit or falls short).

The focus on physical damage or injury is again obvious here, since, even if the desired damage and injury does not come about, the behaviour will still be considered violent despite its failure to have a harmful effect. One aspect that seems vague, in this latter definition, however, is the fact that subsection (b) seems to be implying that an act can be violent, even if the effect of injury or damage or the intent to injure or damage are lacking, yet the act has the potential to cause such effects, even if it did not. This definition seems to define violence, having as a starting point that the act should entail a risk of causing injury or damage.

Greenawalt defines violence as: 'acts of force against persons that cause death, substantial physical pain, or impairment of physical faculties or that restrain physical liberty for a significant period of time, and acts of force against property that destroy or gravely

[131] ibid.

[132] U.S.C., Title 18, Part I, Chapter I, Section 16.

[133] (c.8)

impair its physical integrity.'[134] Although perceptions of the degree of force or the nature of the acts that constitute violence might be different according to different contexts, Greenawalt's definition relates to CD more particularly and focuses on the consequences that suggestions of non-violence were meant to prevent. However, what is apparent is that all definitions relate to physical force, supporting the presumption that the traditional notion precludes the possibility of non-physical violence.[135]

Defining violence as strictly physical would in most cases resolve the need to discuss non-violence in the context of hacktivist actions, the effects of which mostly take place online without any actual physical damage to people or property. Hardware is almost never damaged and software is often restorable as it was before the attack. On the Internet, citizens only deal with abstract, electronically structured representations of physical entities, therefore, eliminating the chance for physical violence.[136] Yar includes as cyberviolent, behaviours that only relate to 'psychological harm or inciting physical harm against others', such as cyberbullying or suggestions inducing offline violence.[137] As for acts that destroy or gravely impair the physical integrity of property, US case-law supports the view that the transmission of unwanted messages, such as spam[138] could be considered physical damage to a computer system.[139] The extent to which the physical damage caused by the spam messages, which might have impaired the functionality of a computer or network, could also be considered violence under the above definitions, however, has not been discussed. One could argue that the relatively low intensity of hacktivist tactics, such as defacements or virtual sit-ins, which can have impairing effects, but are very rarely actually destructive,[140] would probably fail to support a claim for violence.

[134] Greenawalt (n 56) 245.

[135] Himma (n 116) 2-3; Calabrese seems to agree on that, characterising as forms of violence only extreme hacking acts that irreparably destroy server files. Calabrese (n 3) 332.

[136] Michael McGuire, *Hypercrime: The New Geometry of Harm* (Routledge Cavendish, Oxford 2007) 80.

[137] Majid Yar, *Cybercrime and Society* (Sage Publications, London 2006) 10-1.

[138] See *America Online, Inc. v IMS et al.* 24 F.Supp.2d 548 (E.D.Va. 1998); As it was argued, 'AOL's loss of good-will when customers complained about the slow and balky operation of their service was an element of actionable damages, above and beyond physical damage to the system itself.' Richard A. Epstein, 'Cybertrespass' (2003) 70 The University of Chicago Law Review, Centennial Tribute Essays 73*,* 81.

[139] De Villiers (n 118) 41.

[140] Stephen Mansfield-Devine, 'Anonymous: Serious Threat or Mere Annoyance?' (2011) 1 Network Security 4*,* 8.

This could be the case, for most acts, even if we accept the inclusion of acts that entail a risk of causing physical injury or damage to property, since even potent virtual sit-ins will not be as severe as to cause damage to the physical aspects of the network, such as servers. Nonetheless, physicality-based notions of violence seem to disregard an important reason for advocating non-violence. This is the preservation of a proportionate harmfulness, when protesting and the demonstration of a respect to the rights of others through avoiding overtly coercive behaviours. The immaterial nature of property and damage online generates the need for a more abstract interpretation of violence that moves beyond physicality and relates, in our case, at least, more to coercive behaviours leading to damage and loss.[141]

3.2.2 Violence as coercive disruption causing damage and loss

In his definition of CD, Power seems to argue for activities which are non-injurious to the person, something, which would relate to the physical aspect of violence, but he also mentions that protests must be realised in ways respectful to the rights of others.[142] We could argue that this element of 'respect to the rights of others' could lead us to highlight a potential dimension of violence that could apply to cyberspace activities as acts that coerce the exercise of rights of others. Since physical violence does not exist or is very difficult to realise through network disruptions, such as those of hacktivists, the requirement of non-violence in cyberspace could, thus, be translated as a need to moderate the cyberprotests' imposition on the rights of others, so as not to be disproportionately coercive in relation to the context of the protest. As argued above,[143] expectations of complete non-violence can be unrealistic and, thus, CD can also entail an element of coercion and still be justifiable, if it retains its initial persuasive character and attempts to induce change primarily through voluntary reconsideration of policies and not as a response to unavoidable coercion.[144] For example, a virtual sit-in could be employed in order to attract attention to a cause and initiate a discussion for change, but if it is realised in ways that totally hinder the

[141] 'Hyperspace is both continuous with and produced out of "normal" space. It therefore retains all the more limited forms of spatial interaction at its core – while simultaneously extending and complexifying them.' McGuire (n 136) 7.

[142] See Part 2.1 Definitions and initial clarifications.

[143] See (n 128).

[144] Mathias Klang, 'Civil Disobedience Online' (2004) 2 Info, Communications and Ethics in Society 75,76-7; John Morreal, 'The Justifiability of Violent Civil Disobedience' in Hugo Bedau (ed), *Civil Disobedience in Focus* (Routledge, London 1976) 130-43, 135-8.

functionality of a webpage for long periods in order to force the desired change as a precondition for stopping the protest, the level of coercion would be much higher and the act less justifiable. Conversely, low coerciveness can serve publicity goals and even facilitate persuasion between protesters and protested, since it reduces conflict, while still being acceptable.[145] This is because the rights that protesters violate, such as property or access to information, are not absolute, and thus, minor infringements could be accepted for promoting higher moral goals.[146]

Morreal acknowledges that justifiable low coercion relating to non-absolute rights could eventually reach a degree that would be similar to what could be considered morally reprehensible violence by assessing the duration and intensity of the effects of the act.[147] As mentioned above, some form of low violence/coercion will always exist in protests, so the question should be not the existence of a hindrance to rights that could prove a nuisance to someone, but whether this nuisance reaches disproportionate levels so as to be felt more as an unavoidable force. Consequently, acts that impinge on rights can be considered violent, when they disproportionately hinder the exercise of rights, such as physical health, pursuit of happiness and enjoyment of property.[148] In the cases of online CD, the rights that can be compromised are the enjoyment of property and potentially the right to free expression and access to information. As McGuire clarifies, for genuine harm to manifest on a cyberspace level, it will have to relate to a practical or functional loss of a valued right or asset that citizens generally take for granted in their online environment and to reduce its capacity to an almost absolute degree.[149] For example, he argues that, if the right of access to the Internet becomes extremely pervasive and a social necessity, even temporary loss of the capacity for remote interaction could be instituted as harm.[150] At least for now, however, permanent connectivity has not attained such importance.

Assessing the impact of the intensity and the duration and, thus, the coercive nature of the protest is also related to potential damage and loss caused by the impairing act, since

[145] Morreal (n 144); Vinit Haksar, 'Civil Disobedience and Non-Cooperation' in Hugo Bedau (ed), *Civil Disobedience in Focus* (Routledge, London 2002) 144-58, 146-7.

[146] Morreal (n 144); Haksar (n 145) 146-7.

[147] Morreal (n 144); For the need of some degree of coercion in CD see Brownlee, 'The Communicative Aspects of Civil Disobedience and Lawful Punishment' (n 97) 181.

[148] Morreal (n 144).

[149] McGuire (n 136) 124.

[150] ibid.

even short-lived protests can potentially cause financial loss. Consequently, the choice of targets becomes especially relevant to assessments of potential coercion, since impairing the functions of certain websites offering critical services to the public could prove harmful, not only to the direct target, but also to the wider public, which might find it impossible to access important public services due to the network-impairing protest. Moreover, the targeting of private actors, such as financial organisations or commercial websites, could produce large amounts of losses with minor disruptions. Consequently, the notion of risk of harm to property as a potential aspect of violent behaviour becomes more pertinent in those cases where private actors are prevented from making use of their resources, through a virtual sit-in crashing a website for example.

The realisation that the existence and degree of violence in CD is contextually-dependent, relative, and not easily measurable as a criterion of justifiability[151] is also consistent with the analogy created above, perceiving violence in the online context as the coercive infringement of property rights online. This re-interpretation of violence could function as a viable alternative regarding notions of non-physical violence, in cases of hacktivism. However, considering an act as violent for CD, at least, involves the question of the degree of infringement of rights of property or physical integrity, which would have to be generally high in order to constitute coercive, and, thus, morally reprehensible violent activity.[152] Low intensity acts, such as short-lived virtual sit-ins or easily healable viruses might be illegal and rights-impinging, but their effects would not be adequately severe or persistent to seriously impact on the moral assessment of these acts of protest. Even in those cases, where we would characterise these acts as violent, it is argued that, when violence has no chance of leading to the injury of a person or the risk of it, it is a priori much less morally reprehensible.[153]

Hacktivist have often demonstrated their non-coercive intentions by employing tactical measures that also relate to the minimisation of harmfulness. Alternatively, there are no reports of infrastructural facilities being targeted and there is usually no additional damage to the computer systems beyond what is required for the protest to be realised, which

[151] Bedau, 'Civil Disobedience in Focus: Introduction' (n 32) 8; Schlesinger (n 111) 956; Raz (n 97) 267.
[152] Quint (n 24) 125.
[153] Greenawalt, 'A Contextual Approach to Disobedience' (n 126) 61-4; Jonathan Simon, *Governing through Crime* (Oxford University Press, Oxford 2007) 154.

usually entails bypassing authorisation controls and the usually easily reversible modification of underlying code for defacements.[154] Additionally, many activities are publicised in advance, allowing for countermeasures or damage minimisation preparations on behalf of the protests' targets[155] – though admittedly recently, hacktions perpetrated by members of Anonymous have used rhetoric that implied that the attacks might have had a more threatening character in order to prevent specific governmental or corporate actions, rather than a symbolic and publicising intention.[156]

Summing up the discussion of the moral limits of violent protesting, the general presumption in relation to hacktivism is that it should generally be considered non-violent if the physicality element is the defining element. Even if the more fitting interpretation of violence online as coercive network disruptions is adopted, hacktivist practices would, on many occasions fall outside its scope in terms of intensity and duration of effects. That does not mean, however, that damage and loss do not play an important role in proportionality and, thus, also morality assessments, shifting the focal point of discussion of justifiability from physical harm and damage to a more abstract notion of coercion in the form of not preventing the exercise of communication rights and also those of commercial interaction, a form of coercion that can entail high amounts of commercial damage and loss that would impact on the moral assessments of hacktivist protests.[157]

3.3 Efficiency and the conflict of speech rights

Another element that relates to retaining the proportionality between harms and benefits deriving from the act of protest is the need of the act of dissent to be realised in a way so as to be perceived by the public and understood as a protest relating to a specific injustice. In

[154] Evgeny Morozov, 'In Defense of DDoS' (*Slate Magazine,* 13 December 2010) <http://www.slate.com/id/2277786/> accessed 20 May 2011, 2; As Vegh reports, hacktivist intrusions in the World Bank servers were deemed to have caused no actual financial loss. Sandor Vegh, 'Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank' in Martha Mccaughey and Michael D. Ayers (eds), *Cyberactivism: Online Activism in Theory and Practice* (Routledge, London 2003) 91.

[155] Samuel (n 3) 81; DJNZ and the Action Tool Development Group of the Electrohippies Collective (n 1) 274.

[156] See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism.

[157] Greenawalt (n 56) 234-5; Damage is a crucial factor for cybercrime legislation and will play a major role in prosecutions. See Ch 4, Part 3.3.1 The focus on damage and loss and the expansion of the scope.

other words, the existence of an obvious, communicated causal nexus between the protest and the cause. Efficiency, as a criterion influencing the moral justifiability of a protest highlights the need for a causal link between the act of dissent and the cause it relates to in the sense of realising a minor injustice as a way to prevent a more major one. Particularly for online CD, due to technological issues, such as the lack of public fora online,[158] efficiency also encompasses a dilemma between the free expression of protesters and that of the targeted actors. Before proceeding to discuss efficiency more particularly, one should, therefore, discuss one crucial precondition for the efficiency of online protests, which is the conflict of speech rights between protesters and their targets.

In contemporary democracies, with all the new possibilities for expression, especially online, from online radio to blogs or social networks, political opinions and dissent could be expressed without employing tactics that impinge on the speech opportunities of those protested against. Websites include content that forms an expressive message on behalf of those running them, be they private or state actors. Hacktivist tactics that impair the functionality and impede access to these websites consequently infringe on the exercise of the expressive rights of those represented behind targeted websites. Especially for private entities, the courts have recognised a right to free expression, both in the US and the EU.[159] However, this right, in the US at least, is only enforceable against the state and not third parties, although the EU has accepted the notion of horizontal application of rights to third parties, meaning that certain rights are applicable in relations between private actors and not just between the citizens and the state.[160] Consequently, there could be legal protection of corporate speech from third party (hacktivist) disruption. Even members of the wider hacker/hacktivist community have criticised activities, such as virtual sit-ins that are used as a way for promoting free speech-related causes, yet the disruptions they cause hinder the expression of those targeted.[161]

[158] Part 1. Free expression and hacktivism.

[159] Bruce Johnson and Ho Youm, 'Commercial Speech and Free Expression: The United States and Europe Compared' (2008) 2 Journal of International Media & Entertainement Law 159; See also *Citizens United v Federal Election Commission* 558 U.S 310 (2010).

[160] Stephen Gardbaum, 'The Horizontal Effect of Constitutional Rights' (2003) 102 Michigan Law Review 387.

[161] Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (Routledge, London 2004) 90-1.

However, the justifying rationale for disruptive forms of hacktivism is that unauthorised acts are perpetrated as an inevitable, and not just preferred, expressive tool that enables users to compensate for the reduced speech opportunities for expressing dissent online, compared to influential elites with extensive mainstream media access.[162] The idea of ‘publicness’ is sensitive in cyberspace, since there are many opportunities for one to express oneself through a personal website, but that expression will normally be restricted to a small circle of friends and peers and will not have the popularity and visibility of more mainstream websites.[163] Therefore, assessing the immorality of hacktivist actions that disrupt the speech rights of their targets ought to take into account the multiplicity of alternative expressive channels that the protesters’ targets have available, compared to the channels that protesters can access. Governments or big corporations often dominate time, space and information distribution on the popular mainstream communicational channels, which leads to manipulating democratic and norm-building processes and, thus, disproportionately influencing socio-political discourses towards their desired directions.[164] Even online Internet service providers often employ personal policies in relation to the speech they allow on their social spaces, while Internet search engines such as Google promote more popular search results thus marginalising minority views.[165] Minorities and alternative political views are often marginalised and lack the capacity to employ similarly popular channels for reaching an audience and communicating their views.[166]

Therefore, efficient communication of the political message on a space that is relevant to the cause of the protest and frequented by the general public essentially requires that it be expressed on third-party websites without authorisation.[167] Hacktivist tactics broaden

[162] Klang (n 144) 82-3; See also Part 1. Free expression and hacktivism.

[163] Lijun Tang and Peidong Yang, 'Symbolic Power and the Internet: The Power of a 'Horse'' (2011) 33 Media Culture Society 675, 676; For example, one can express dissent in a personal blog, but the number of readers is ultimately related to the general media influence of this person and its being linked to by more major and popular media. Therefore, although essentially public, the blog has the potential to reach a small amount of people in the wider public. The way for dissidents then to reach the wider public that interacts with their protest targets is to take their speech and dissent to the websites of their targets, which will often be more popular and closely related to their cause.

[164] Manuel Castells, *Communication Power* (Oxford University Press, Oxford 2009) 298; Scott Burris, Michael Kempa, and Clifford Shearing, 'Changes in Governance: A Cross-Disciplinary Review of Current Scholarship' (2008) 41 Akron Law Review 1, 28.

[165] Stephanie Winston, '“Don’t Be Evil”: Uncovering the Implications of Google Search' (2011) 7 Dalhousie Journal of Interdisciplinary Management 1; Nunziato (n 18).

[166] Castells, *Communication Power* (n 164) 298; Burris, Kempa, and Shearing (n 164) 28.

[167] See 1. Free expression and hacktivism.

the scope and diversity of expression and social debate by offering the opportunity to speak on the same popular space with those hacktivists protest against, mainly states and corporations and, consequently, they gain access to similar amounts and types of audiences.[168] Assessments of morality ought to evaluate each particular context, in relation to the speech opportunities of each side of the conflict and the overall level of impact of hacktivist protests on the sum of speech opportunities of the protested parties.

However, the moral evaluation of hacktivist actions that is based on the existence of an obvious and strong protest/cause nexus can be problematic. This is because the implicit symbolic nature of indirect CD tactics might obscure the clarity of the protest message and, consequently, the protest act's relation to the injustice protested. The absence of an obvious effect and, thus, a causal link between protest and goal can render the law-breaking protest less effective in terms of it being registered as an appeal to a just cause and, consequently, in terms of its contribution to remedying the injustice. When the causal link between protest and goal is obscured or too vague, moral assessments based on a balancing of benefits and harms may result in the protest being considered excessively harmful compared to its actual contribution to remedying the injustice.[169]

In relation to the issues of clarity and actual impact, hacktivist tactics, such as virtual sit-ins, can sometimes prove inefficient, breaking the law without any actual speech effect being registered, if the disruption is countered by the targeted site or is not so potent as to attract public or media attention. Even if some form of temporary disruption is generated it could be perceived as a technical problem. However, even protests such as redirects where the effect is registered, could be of doubtful efficiency. Despite the general efforts to publicise protests in advance, so that the actual nature of a potential disruption is registered by the public, especially for virtual sit-ins, the potential low popularity of alternative media that promote hacktivist events could result in the actual message of the protest reaching only small audiences.[170] The same could apply to viruses countered by antivirus programs. The example of virtual sit-ins best highlights the conflict between

[168] Samuel (n 3) 210-2.

[169] Carl Cohen, 'Civil Disobedience and the Law' (1966) 21 Rutgers Law Review 1, 4-5; Hugo A. Bedau, 'Civil Disobedience and Personal Responsibility for Injustice' (1970) 54 The Monist 517.

[170] Jordan and Taylor (n 161) 79-80; 2600 Magazine, 'Press Release - 2600 Magazine Condemns Denial of Service Attacks' (*2600 Magazine,* 10 December 2010) <http://www.2600.com/news/view/article/12037> accessed 27 October 2012.

efficiency and harmfulness, since hacktivists will often have to find ways to balance between generating an adequate level of disruption to be noticeable, yet also not be as disruptive so as to be considered disproportionately coercive and harmful to speech and property. For example, even though prior announcement of a protest might reduce its disruptiveness and potential harmfulness, as it would give the target site time to prepare a defence, notification would also compromise the actual disruptive effect of the protest, if it were countered by the prepared defences.[171]

Concerns about the potential efficient promotion of a political cause by the hacktivist protests' effects are indeed valid. However, expecting immediate effects from hacktivists would regard hacktivist practices, wrongly, as isolated phenomena, disconnecting them from other on- and offline efforts towards the same goals.[172] After all, the usual aim of CD and hacktivistm is to publicise injustices and sensitise the actors engaged, being only parts of wider socio-political, multi-action struggles that function in a mutually reinforcing way and form a continuum of struggle, with multiple efforts aiming to achieve the same goal.[173] Hacktivists usually try to establish causal links between their actions and the causes they support by choosing to target popular websites that are contextually related to the cause promoted, and by combining their actions with real-life protests.[174] Furthermore, despite the danger of not being noticed by the public, if the disruption is countered or participation is low, as mentioned above, in cases where multiple users are engaged in the protest, such as virtual sit-ins or a voluntarily shared artistic virus, these efforts can still be politically mobilising and engaging, as they can often be supported by hundreds or thousands of

[171] An example of this is the protest against Lufthansa, where the company had been notified in advance and had taken precautionary measures in order to absorb the increased traffic with less disruption. See (n 24).

[172] For example virtual sit-ins in Seattle were part of a very complex campaign against the World Trade Organisation meeting – see: Ian Walker, 'Interview: Naomi Klein' (*ABC,* 2001) <http://www.abc.net.au/tv/hacktivists/klein_int.htm> accessed 20 October 2010.

[173] Pamela E. Oliver, 'Bringing the Crowd Back In: The Non-organizational Elements of Social Movements' (1989) 11 Research in Social Movements, Conflict and Change 4, 7-8.

[174] Jordan and Taylor (n 161) 152-3; Bruce Simon, 'Illegal Knowledge: Strategies for New Media Activism: Dialogue with Ricardo Dominguez and Geert Lovink' in Bousquet Marc and Wills Katharine (eds), *The Politics of Information: The Electronic Mediation of Social Change* (Altx Press 2003) 55-65, 58-9; See, for example, use of hacktivism in struggles against the Iranian regime and the global support these protests generated. Jon Leyden, 'Iranian Hacktivists Hand-Crank DDoS Attack' (*The Register,* 22 June 2009) <http://www.theregister.co.uk/2009/06/22/iranian_hactivism/> accessed 20 October 2010.

people.[175] As Denning argues, the protesters' cause can be communicated, not just through the crashing of the website, but also due to the mass engagement of citizens, even without any major network interruption.[176] Moreover, other hacktivist tactics, such as defacements, might be mirrored by many users in social networking sites and, thus, achieve greater publicity and communicate the message more effectively. After all, the actual impact of a hacktion, both short- and long-term, cannot be foretold or gauged easily, as it also relies on external elements, complex, large-scale events and slow political processes.

Therefore, the relativity of this criterion and the interplay of efficiency with the problems of speech and proportionate disruption could lead one to conclude that moral justifiability would have to be linked with the intended effectiveness and causality between targets and protested cause and not the existence of an immediate effect and political change. Protesters should, therefore, make choices that would render the protest as relevant as possible to the cause in terms of targets, tactics and communicated messages. The actual disruptive outcome, which can rely on pure luck or even unanticipated countermeasures from the protested side,[177] should not greatly impact on assessments of morality, unless it reflects an intentional effort of the protesters to cause disruption without any causal relation to an injustice or any underlying message.

3.4 Acceptance of punishment

Another important element affecting the justifiability of CD and relating to the protesters' demonstration of respect for the legal order they operate in is the acceptance of punishment by the protesters. This requirement is considered indicative of the protesters' self-sacrificial, altruistic intentions and their respect for their political regime and their co-citizen rights, which are compromised by their law-breaking.[178] Moreover, the openness of

[175] Ricardo Dominguez, 'Electronic Civil Disobedience' (*thing.net,* undated) <http://www.thing.net/~rdom/ecd/ecd.html> accessed 16 January 2011.

[176] Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Jon Arquila and David Ronfeldt (eds), *Networks and Netwars:The Future of Terror, Crime, and Militancy* (RAND Corporation, 2001) 266-7.

[177] Defensive measures on behalf of a protested website could allow it to absorb the traffic of a virtual sit-in and, thus, render the protest invisible to the media and wider public. However, the effort would be publicised online before and after by the protesters.

[178] Herbert J. Storing, 'The Case against Civil Disobedience' in Hugo A. Bedau (ed), *Civil Disobedience in Focus* (Routledge, London 2002) 86; Stephen R. Alton, 'In the Wake of Thoreau: Four Modern Legal

identity that an expectation to accept punishment presupposes is also a justificatory factor, because it ensures the public nature of the protest and distinguishes protests from covert criminal acts, essentially confirming the moral intentions of the protesters.[179]

Nevertheless, the interpretation and true implications of such a moral requirement have been strongly contested. As Arendt argues, society cannot expect from the disobedient to accept punishment, since that would require of her not to defend her case, consequently, nullifying her basic defendant rights.[180] Although Gandhi and Raz have argued that accepting punishment is linked with the state's acknowledgment of the moral motives of the protesters and with the imposition of lenient penalties, they find it unlikely that the authorities will ever accept any potential legitimacy of the protesters' cause.[181]

However, this criterion should not be interpreted narrowly to mean that protesters should seek and accept whatever punishment is handed down. Acceptance of punishment relates more closely to the protesters expressing their dissent publicly and being identifiable and traceable in order to be tried, if the public order sees a need for it. These aims, however, could be equally served through a moral expectation that the disobedient should do nothing to actively avoid the risk of arrest and prosecution;[182] an interpretation which resolves the problems that an unqualified acceptance of any punishment creates. The acceptance of, at least, the prospect of arrest and punishment by protesters could function as a guarantee that alleviates public frustration caused by the protesters' law-breaking and also tests the protester's conviction in the legitimacy of his cause.[183] Adopting the acceptance of the risk of prosecution rather than of punishment, as a moral criterion, also avoids the judicial unreasonableness of expecting the protesters not to pose any legal defence in court.

Instead, acceptance of the prospect, rather than the punishment per se, will allow the protester to defend her case properly and publicise the justness of her cause and allow her

Philosophers and the Theory of Non-Violent Civil Disobedience' (1993) 24 Loyola University Law Journal 39, 63-4.

[179] Greenawalt, *Conflicts of Law and Morality* (n 56) 238-40.

[180] Arendt (n 59) 54-55.

[181] Haksar 'The Right to Civil Disobedience' (n 119) 421-2.

[182] Woozley (n 128) 330.

[183] Greenawalt 'A Contextual Approach to Disobedience' (n 126) 69-71.

to remain politically active.[184] Therefore, acceptance should not be read as acceptance of the specific punishment handed down by courts, but instead acceptance of the prospect of being faced with sanctions for their activity and also their need to defend their actions and justness of cause in court. This course would, consequently, avoid the delegitimisation of just causes and the elimination of the politically sensitised part of society, which could result from an unquestioning acceptance of any punishment.[185] The state would, instead, have to convince the court that it has good reasons to punish these protesters who have beliefs so strong as to risk punishment for them.

This alternative reading of accepting the risk of prosecution would be consistent with how cyberspace protests are realised and the specific difficulties of identifiability in cyberspace, where, prima facie, anonymity and distance create difficulties in locating, apprehending and punishing deviants.[186] From the Internet's inception, anonymity has been the standard norm and has generated and facilitated criminal behaviours, but also the more acceptable values of privacy, freedom of expression and creativity and is, therefore, deemed worthy of preservation.[187] Hacktivists have adopted varying degrees of identifiability, from full openness to full covertness, which are related to their degree of acceptance of accountability and influence their moral legitimacy.[188] The more politically mature groups publicise their identities or use traceable pseudonyms,[189] while members of the Electrohippies argued that total exposure of identity could endanger their livelihoods

[184] Colby (n 129) 1173-4; However, in direct disobedience one might object to punishment, since he considers the law disobeyed should not exist in the first place.

[185] ibid.

[186] Ch 4, Part 3.4 Resources, information and lack of harmonisation.

[187] Joseph M. Kizza, *Ethical and Social Issues in the Information Age* (Springer-Verlag, New York 2010) 83; Katja F. Aas, *Globalization & Crime* (Sage Publications, London 2007) 156; Lawrence Lessig, *Code v.2.0* (Basic Books, New York 2006)18-20, 190-2; '[...]disassociation and lack of physical proximity encourages people to participate in illegal activities in the Internet, such as hacking, denial of service[...]. They do not feel that in reality they are doing any serious harm.'; Gregor Allan, 'Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative' (2005) New Zealand Law Review 149, 175-6.

[188] These can range from total anonymity to open declaration of identification: Samuel (n 3) 214-5.

[189] ibid; See the transparency policies of EDT and pseudonymity of Electrohippies in Jill Lane and Ricardo Dominguez, 'Digital Zapatistas' (2003) 47 TDR 129; DJNZ and The Action Tool Development Group of the Electrohippies Collective (n 1) 274; Even Anonymous, who generally advocate anonymising techniques, employ software that allows IP-tracing and cannot be used through anonymising websites, eventually resulting in detection and prosecution of protesters. Mansfield-Devine (n 140) 6; Bob Garfield, 'In Defense of DDoS' (Transcript of interview with Evgeny Morozov, *On the media,* 17 December 2010)<http://www.onthemedia.org/transcripts/2010/12/17/02> accessed 20 May 2011; 'Unlike fingerprints, IP logs cannot specifically designate the person that was using that IP address. Law-enforcement will have to use real-world evidence to eventually find the last user of the terminal of interest.' Allan (n 187) 151-2.

due to potential social and workplace prejudice towards their activities, without substantially facilitating their traceability by the authorities.[190] After all, constantly evolving technologies of control in cyberspace have ultimately rendered anonymity difficult to achieve, especially for everyday users that lack the willingness or knowledge to employ 'anonymisation' techniques.[191] As Lessig argues, the trend towards extreme identity-authentication technologies on the Internet is unstoppable, especially since Internet infrastructure has the potential to facilitate the development of such techniques.[192]

Consequently, it would seem that difficulties in potentially apprehending protesters, even the more technically-capable hacktivists, often seem to be more an issue of resource-availability or discretion on behalf of law-enforcement agencies, rather than flowing from hacktivists' attempts to avoid apprehension. Virtual sit-in tools, for example, have exposed the IP- addresses of protesters that were then prosecuted for their protests. However, due to the serious charges and high penalties that hacktivists currently face that far exceed those faced by normal CD protesters, hacktivists have recently considered or employed anonymity measures more extensively, despite the implications for the moral justifiability of their acts.[193] Nevertheless, the traditional norm integrated into the virtual sit-in tools and the practices of the early era of hacktivism is that protesters would often refrain from totally masking their identities and would instead be more easily locatable by law officials. This practice should be considered adequate proof of trust in the legal system and of moral intentions of the protesters, thus, reinforcing the protesters' moral justifiability. The above interpretations of openness in conjunction with the acceptance of punishment through identifiability seemingly reconciles the citizens' desire to know protesters could be sanctioned, if required, with the need of protesters to demonstrate a basic respect for the legal system, but also retain some sense of privacy in relation to their expressive actions.

[190] Klang (n 144) 81.

[191] Lessig (n 187) 203; Constance Zhang, 'Regulation of the Internet-New Laws and New Paradigms' (2006) 17 Journal of Law, Information & Science 53, 67-8. Morozov has also emphasised how social media and the Internet in general can also facilitate the tracking down and deterrence protests and how new technologies of surveillance have struck a serious blow to the early year presumptions that the Internet was a place of deliberate, impenetrable anonymity: Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs, New York 2011); See the counterargument in Trevor Thompson, 'Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the White Hats under the CFAA' (2008) 36 Florida State University Law Review 537*,* 547-8.

[192] Lessig (n 187) 45-6.

[193] For example, the radicalisation of persecution has led members of Anonymous to consider more radical tactics regarding anonymity. See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism. Radicalisation will be discussed more in the following chapters.

3.5 Last resort

Theorists have argued that CD should be used only as a last resort after the exhaustion of all legal alternatives in order to demonstrate a belief in the legal democratic means of amelioration.[194] This moral requirement also expresses the essence of proportionality, where the choice of means should be the least damaging possible to achieve the desired result.[195] This particular requirement would, thus imply that, if all the other equally efficient legal remedies are not exhausted, recourse to law-breaking would be disproportionately harmful per se and therefore immoral in a democratic regime, where there are usually legal political means available for seeking redress. This demand is nowadays reinforced, not only by the fact that, in contemporary democracies, free political expression is considered strongly established,[196] but also by the novel expressive opportunities of digital technologies, which allow citizens to create their own content through blogs and other online platforms. Arguably, the various different legal means of expression and political participation are considered adequate for facilitating political dissent and change, consequently, rendering all illegal acts of protest disproportionate, and thus, less justifiable.[197]

However, this requirement fails to acknowledge the potential deficiencies in formal law-making and accountability processes, such as capture of political processes by lobbying interests or the increasingly governing role of private actors that do not have to abide by constitutional standards of review.[198] Furthermore, such a requirement seems to disregard

[194] Rawls, *The Theory of Justice* (n 28) 327-8; Merton Tice, 'Civil Disobedience: A Study of Law and Its Relation to Society' (1968) 13 South Dakota Law Review 356*,* 361; Lasse Thomassen, 'Within the Limits of Deliberative Reason Alone: Habermas, Civil Disobedience and Constitutional Democracy' (2007) 6 European Journal of Political Theory 200, 203.

[195] Greenawalt, 'A Contextual Approach to Disobedience' (n 126) 61.

[196] The First Amendment in the US Constitution and articles 10(free expression) and 11(assembly) incorporated in the UK Human Rights Act of 1998 legally guarantee these rights for all citizens. See also Part 1. Free expression and hacktivism.

[197] Himma (n 104) 4-5; US courts have supported there can be a presumption that petition and elections could always bring change legally, rendering the potential exhaustion of legal means impossible. See: Cohan John A. Cohan, 'Civil Disobedience and the Necessity Defense' (2007) 6 Pierce Law Review 111*,* 141-2.

[198] Castells documents the power imbalances in modern information society democracies. Castells, *Communication Power* (n 164); Black also discusses the deficiencies of state regulatory processes and agencies, suggesting the need for regulation to move beyond the core democratic state: Julia Black,

cases where legal means of protest could have more serious social effects than illegal ones.[199] The relative nature of such a requirement is more evident, when acknowledging the common fact that judicial and legislative mechanisms are overburdened in most countries and initiating proceedings can be very slow and costly.[200] Citizens might arguably even resort to CD due to unsuccessful and arduous efforts to gain access to formal legal remedies.[201] Where the injustice is current and ongoing, and has persisting consequences for a social group, these inefficiencies are further emphasised.

Although moral theories on disobedience would converge on the fact that when obviously accessible and possibly effective legal alternatives exist, political law-breaking should not be resorted to lightly, the requirement to exhaust all possible legal remedies could constitute an insurmountable moral demand on acts of CD and hacktivism.[202] This requirement, perceived strictly as a requirement to exhaust any possible means of legitimate protest, would often practically overburden protesters, as they would be expected to sacrifice time and resources in pursuing bureaucratic, institutionalised and potentially inefficacious processes. Especially in an era when politics have transcended national sovereignties and are formulated by international groups[203] and financial organisations,[204] this requirement becomes untenable in its absolute form. Therefore, the strictness with which one should assess the morality of CD in relation to the existence of alternative, less harmful means of amelioration ought to relate to the particular context and the accessibility or potential success of legal means. Both Rawls and Greenawalt, for example, acknowledge that in cases of urgency or when the legal options appear potentially fruitless, the ultimate resort criterion should be ignored when assessing the morality of the protests.[205]

'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1; Schwarz (n 127) 558-9;

[199] A strike of ambulance drivers would most probably generate more social distress than a virtual sit-in on the website of the Ministry of Health: Raz (n 97) 269.

[200] Kellner (n 111) 904.

[201] ibid 903-4; Arendt (n 59) 74; An example is when strongly supported petitions are ignored without due consideration.

[202] Cohan (n 197) 141-3; For example, in *US v Schoon,* 22 Ill.971 F.2d 193 (9th Cir. 1991)(*Schoon*), the Court argues that even the possibility for Congress to change its mind on an issue was sufficient to satisfy a reasonable assessment on the existence of legal alternatives.

[203] Examples are the European Commission or the United Nations Security Council.

[204] World Trade Organisation in Africa, International Monetary Fund in Greece, Argentina, Romania.

[205] Greenawalt (n 56) 229; Rawls, *The Theory of Justice* (n 28) 327-8;

Hacktivism expresses, at least partly, the popular frustration for a gradual increase in inaccessibility or inefficaciousness of formal means of amelioration in contemporary democracies. Hacktivist projects bring together people globally in protests against social matters for which the legal remedial means are often beyond their jurisdictional or financial reach, despite the global implications of the political acts protested. For example, the act of Visa and Paypal to arbitrarily freeze donations towards Wikileaks, despite there not being a criminal charge against the organisation, was considered an act with political dimensions that had a serious censoring impact on speech online.[206] Naturally, few will have the resources to take to court such a decision with global implications on speech and the slow court proceedings could financially exhaust Wikileaks.[207] Considering that the protests and the subsequent publicity eventually reversed the decision of Paypal to block donations to Wikileaks,[208] one could see how protesting after all legal remedies have been exhausted could have made the protests meaningless.[209] Moreover, hacktivism, with its usually provocative, eye-catching nature could act as a precursor to the employment of legal measures of amelioration by generating public discussion bringing the issue to the fore of even global mainstream media.

The need for careful consideration on behalf of protesters before the employment of illegal means of protest is a valid concern, in order to avoid the full substitution of legitimate democratic procedures by unprincipled and generalised vigilantism in the form of disproportionately coercive protests. However, moral assessments of CD should take into account the actual contemporary political conditions in relation to the possibility of access and success of prior legal means. Such an evaluation process would entail assessing whether legal recourse was possible, accessible and potentially efficient, whether such

[206] See Yochai Benkler, ‘Free Irresponsible, Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate’ 46 Harvard Civil Rights-Civil Liberties Law Review, 311, 331-2.

[207] Wikileaks argued that after the donations froze, they witnessed a revenue drop of 95%: Alex Fitzpatrick, 'Wikileaks Wins Battle against Visa, Mastercard' (*Mashable,* 12 July 2012) <http://mashable.com/2012/07/12/wikileaks-wins-battle-against-visa-mastercard/> accessed 10 June 2013.

[208] Charles Arthur 'Inside 'Anonymous': Tales from within the Group Taking Aim at Amazon and Mastercard' (*The GuardianTechnology Blog,* 13 December 2010) <http://www.guardian.co.uk/technology/blog/2010/dec/13/hacking-wikileaks> accessed 19 June 2013.

[209] Fitzpatrick (n 207) The legal battle between Wikileaks and Visa for restoring their service to Wikileaks was decided more than a year after the processing of donations was suspended.

measures have been sought prior to employing illegal ones and whether CD could function as a way to activate these legal processes.[210]

These assessments connect the justifiability of protesters to third-party actions, yet it would be meaningless to demand that every protester employ the same legal remedies, since consecutive court proceedings on similar legal bases would just delay more urgent actions.[211] The coordination of remedial means can also be linked to the expectation of coordination and consequently minimisation of CD that Rawls argues, since an assessment of the potential measures already taken, both legitimate and illegitimate, could result in more coordinated action on behalf of different groups pursuing similar goals. Although coordination might be difficult in relation to causes that have a global impact or relate to many different groups with different agendas, the new, technology-facilitated and globally communicating political movements could perhaps demonstrate some degree of coordination, even at an international level for the promotion of global causes. Anonymous, being a globally accessible and all-encompassing collective, despite its decentralised nature, could arguably satisfy the need for merging disobedient acts and groups into unified efforts through their coordinated acts, which would be organised on their publicly accessible Internet fora.

4. Conclusion

This chapter has evaluated the potential for hacktivism to be considered morally justifiable. It first discussed the links between free expression and hacktivism and the reasons why symbolic hacktions cannot be considered identical to protected free speech due to their law-breaking aspect, despite the strong links of these activities to free expression. Subsequently, the analysis focused on assessing the moral justifiability of CD and the analogies drawn between the reasons for justifying CD and hacktivist practices. The discussion led to the distillation of some indicative criteria that influence the moral

[210] Cohan (n 197) 142-3; Eric Engle, 'The Rights' Orchestra: Proportionality, Balancing, and Viking' (2011) New England Journal of International Law and Comparative Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1704503> accessed 11 January 2013; Although the US approach is called means-ends rational review, the elements examined are similar.
[211] Cohan (n 197) 143.

justifiability of CD, such as non-violence, acceptance of punishment, the need for a conscientious belief that an injustice exists and an efficient causal nexus between protest and cause, and even the prior consideration of employing legal means.

The analysis reviewed these criteria and their applicability in contemporary society and discussed the ways in which hacktivists can or should be expected to satisfy such criteria in order to establish and enhance their moral justifiability. What this process demonstrated was that hacktivism, as a political expressive practice, has the potential to satisfy the identified criteria to a large extent, if not absolutely, when these are interpreted in accordance to current socio-political conditions and the changes in perceptions that the characteristics of hacktivism introduce.

However, the theories discussed in this chapter also led to one more important, overarching conclusion: according to the theories of justice discussed, the criteria extracted and the analogies drawn, one can see that there are degrees of justifiability for different actions and in different contexts. Not all hacktivism is a priori completely criminal or totally justifiable and, in many cases, deciding on the justifiability will be a challenging assessment process. However, the aim of this chapter was to demonstrate that hacktivism can indeed satisfy moral criteria that justify offline CD and can, thus, acquire a similar degree of political legitimacy, as that suggested for CD, despite the obvious illegality and expressive quality of both.

The establishing of the moral justifiability of hacktivism will also form the basis for arguing whether the current approach is problematic considering the character of hacktivist acts that highlights a need for contextual, discretionary and potentially more lenient approaches according to those supporting the justifiability of these acts. DeForrest is of the view that CD should be attributed a ‘legitimate yet informal place’ in the polity.[212] Habermas submits that the democratic state should first acknowledge the conflict between political legitimacy and illegality inherent in CD and prosecute, if necessary, but must simultaneously recognise in the civilly disobedient as a guardian of its own legitimacy.[213] Raz also argues that the courts should take weighty moral reasons for lawbreaking under

[212] DeForrest (n 130) 654.

[213] Habermas and Calhoun (n 61) 137.

consideration, even if these justifications are not formally included in the law, in the form of justification defences.[214] Similarly, Hampson argues that 'forms of hacktivism that are primarily expressive, that do not involve obtaining or exploiting illegal access to computers or networks for commercial advantage or financial gain, and that cause little or no permanent damage, should receive at least some protection as a legitimate form of protest.'[215]

The next chapter will discuss how the moral justifiability of these activities impacts upon the arguments for justifying criminal punishment, both in terms of effective prevention of criminality as well as restoring the balance of justice disturbed by the law-breaking by handing down just punishments. This analysis will further demonstrate why harsh criminal punishment might be a problematic measure to be employed as a predominant tool for hacktivism and will assess the compatibility of criminal punishment rationales to the criminal punishment of hacktivism in order to further establish the general need for criminal sanctions to take a secondary role in dealing with such activities, either due to lack of efficiency or due to justice considerations. The resulting conclusions from these two chapters will inform the criticism of the current regulatory conditions that will follow and the final suggestions for improving the regulation of hacktivism.

[214] Raz (n 97) 236-7.
[215] Hampson (n 7) 531-2.

CHAPTER 3
HACKTIVISM AND THE JUSTIFICATION OF CRIMINAL SANCTIONS

The previous chapter discussed the justifiable nature of civil disobedience (CD) and hacktivism as a form of electronic civil disobedience (ECD) and the moral criteria that influence this justifiability. The justifiability of these political activities has induced theorists to suggest that CD should be attributed a 'legitimate yet informal place' in the polity,[1] and the established analogy between CD and ECD would suggest that similar expectations could be expressed for hacktivism, if similar moral criteria of justifiability are followed for ECD. This acceptance of moral political law-breaking as a legitimate political activity is also interpreted as a call for leniency or even tolerance and milder sanction to no punishment or resort to alternative sanctions than those designated for criminals.[2] This can be realised, for example, through the discretion of prosecutors not to prosecute or to suggest lower penalties and courts to hand down lower punishments or juries to acquit.[3]

However, calls for leniency and tolerance based on abstract political arguments could not be considered self-evident, since they are not commonly accepted, when discussing the potential liability and punishment of CD and ECD. Theorists, for example, have supported full criminal punishment for CD and hacktivists, analogising these activities to plain criminality, if not terrorism.[4] As has been seen in Chapter One, there is no doubt that even the tactics that have been considered morally and politically legitimate (defacements, sit-

[1] Mark E. DeForrest, 'Civil Disobedience: Its Nature and Role in the American Legal Landscape' (1998) 33 Gonzaga Law Review 653, 654.

[2] John Rawls, *The Theory of Justice* (Harvard University Press, Cambridge 1999) 339; Juergen Habermas and Martha Calhoun, 'Right and Violence: A German Trauma' (1985) 1 Cultural Critique 125, 137; Robert Hall, 'Legal Toleration of Civil Disobedience' (1971) 81 Ethics 128*,* 132-3.

[3] Hall (n 2) 132-5; The ways for exercising discretion and how they currently function will be analysed more extensively in the next chapter.

[4] See Habermas and Calhoun (n 2) 127-9; Stuart M. Brown Jr, 'Civil Disobedience' (1961) 58 The Journal of Philosophy 669*,* 672; For hacktivism: Dorothy Denning, 'Hacktivism: An Emerging Threat to Diplomacy' (2000) 77 Foreign Service Journal 43; for recent anonymous virtual sit-ins being considered anarchist or terrorist acts see Crosstalk, 'From Hacktivism to Wikiwarfare' (*RT,* 17 December 2010) <http://www.youtube.com/watch?v=mFJa9RHAfOk> accessed 19 Decemeber 2012; Tim Black, 'Hacktivism: The Poison Gas of Cyberspace' (*Spiked-Online,* 14 Decemeber 2010) <http://www.spiked-online.com/index.php/site/article/10001/> accessed 14 December 2010.

ins) are, prima facie at least, illegal. Therefore, actually assessing the level of sanctioning and the justifiability of these sanctions in relation to the special moral characteristics of online protests requires further legal analysis. This chapter will thus focus on analysing whether and how the political arguments for leniency could be translated into legal arguments in relation to the justifying reasons that society resorts to criminal punishment.

Whether leniency and tolerance are appropriate for CD and ECD that are realised based on moral criteria will be assessed by comparing the justifying reasons for punishment against the moral and socially beneficial characteristics of these political protests. The conflict between justifications of ECD and justifying reasons of criminal punishment will gradually unveil the appropriate type and extent of punishment for dealing with these activities based on the goals of preventing crime and maintaining a balance of justice and proportionality in punishment. In order to better understand the following analysis, though, some preliminary clarifications should be made for the process of criminalisation and punishment.

1. Criminalisation and punishment of ECD as a continuum

1.1 From criminalisation to conviction

Hacktivist tactics fall within the scope of cybercrime laws for unauthorised access and damage to computer systems and conspiracy, offences that can have a maximum penalty of 15 years.[5] Understandably, hacktivists would rarely be given the maximum penalty, yet being accused of such a serious offence with such a broad penalty range immediately increases the potential sanction for them. Moreover, ECD could potentially be prosecuted under provisions that connect cybercrime provisions with counter-terrorism laws, thus, significantly raising the ultimate level of punishment.[6]

Proscribing certain behaviours as criminal, however, expresses the legislature's initial judgment that particular actions are generally socially harmful and reprehensible and is

[5] Ch 4, Part 3.3 The dominating provision of computer damage.

[6] Ch 4, Part 3.3.4 Hacktivism and the link with cyberterrorism.

only the first necessary step of attributing punishment.[7] The administration of criminal justice goes through various subsequent processes and assessments before the suspect is finally penalised or acquitted.[8] Ultimately, the verification of the punishable character of a specific act is decided by the executive (law-enforcement) and the courts (judges and juries), which are burdened with evaluating the specific facts of each case in relation to the actual need and extent of punishment.

1.2 Punishment and the need for specific justification

Punishment has been characterised as a stigmatising and distressing deprivation of the rights of the offender that is imposed publicly by the state.[9] Being an imposition on citizen rights by the state, punishment must be founded on strong justifying aims, since it essentially opposes the purpose of contemporary democracies as protectors of citizens' well being, while at the same time aims to protect the rights of other citizens.[10] Arguably, punishment should be considered 'something that we never get right'[11] and that is why its imposition should be founded on a combination of justifying reasons, 'because no single set of assumptions or beliefs is capable of putting our doubts to rest.'[12]

The justification of penal policies has been considered reliant on the existence of two main qualities: 'that it is morally legitimate and that it has sufficiently compelling rationale [...] we must look to the categories of the Right and Good and we must be satisfied that it violates no principles of right and that it accomplishes some Good.'[13] Therefore, being a state-imposed harm, punishment draws its legitimacy from maintaining/restoring a balance of justice (Right), but also from the utility of accomplishing a socially beneficial result

[7] Nikolaos Androulakis, *Penal Law: General Part* (P.N. Sakkoulas, Athens 2000) 65-66.

[8] Samuel Walker, *Taming the System: The Control of Discretion in Criminal Justice, 1950-1990* (Oxford University Press, Oxford 1993) 6.

[9] John Kleinig, *Ethics and Criminal Justice: An Introduction* (Cambridge University Press, Cambridge 2008) 196; Kimberley Brownlee, 'Justifying Punishment: A Response to Douglas Husak' (2008) 2 Criminal Law and Philosophy 123, 124. Ted Honderich, *Punishment: The Supposed Justifications Revisited* (Pluto Press, London 2006) 4, 8.

[10] Erik O. Wright, *The Politics of Punishment: A Critical Analysis of Prisons in America* (National Criminal Justice Reference Service Library Collection Harper & Row Publishers, New York 1973) 22.

[11] Bonnie Honig, 'Rawls on Politics and Punishment' (1993) 46 Political Research Quarterly 99, 121.

[12] John Gardner, 'Crime: In Proportion and in Perspective in Andrew Ashworth and Martin Wasik (eds), *Fundamentals of Sentencing Theory* (Clarendon Press, Oxford 1998) 32.

[13] Jacob Adler, *The Urgings of Conscience: A Theory of Punishment* (Temple University Press, Philadelphia 1992) 13.

(Good). It is consequently, relying on both deontological and consequential considerations, which are intrinsic elements of a state's legitimate penal policy.[14]

Although many different interpretations of the justifying reasons of punishment exist,[15] this discussion will focus on the two prominent categories of justification: utilitarian crime prevention and just deserts. This narrowing down will enable a more manageable, yet inclusive, analysis, in terms of length and understanding, but will also enable a sufficiently detailed account of the relation between hacktivism and the two pillars of current punishment justifications. The following section will explore the utilitarian prevention of crime in order to examine the tactics of crime prevention and to demonstrate how they should be geared towards promoting social utility. Subsequently, I will try to assess whether the attempt to achieve prevention through strict punishment, usually translated as long periods of incarceration would be efficient and would promote social utility more than more lenient penalties. If it can be shown that lower penalties would have equally efficient preventive effects, while causing less harm to offenders and the general public, then the suggestions for leniency can be considered more appropriate based on this theory.

2. Punishment Justification: Forward-looking theories: Utilitarian crime prevention

2.1 Utilitarian prevention and punishment

Utilitarian prevention theories justify punishment due to its production of good results and the prevention of bad ones; hence, they are called forward-looking theories.[16] The main ways prevention is sought are deterrence, incapacitation and reform/rehabilitation. This

[14] Justice has been considered an essential characteristic of political activities and it is also a feature citizens deem crucial in criminal justice policies. John Rawls, *The Theory of Justice* (n 2) 193; Paul. H. Robinson, 'Why Does the Criminal Law Care What the Layperson Thinks Is Just? Coercive versus Normative Crime Control' (2000) 86 Virginia Law Review 1839*;* Moreover, criminal justice also has certain social goals, since governmental policies should also have a practical, public welfare aspect, such as crime prevention. Honderich (n 9) 87.

[15] For a collection of the various interpretations offered for forward and backward-looking justifications of punishment see Honderich (n 9).

[16] Edward W. Strong, 'Justification of Juridical Punishment' (1969) 79 Ethics 187, 188; Honderich (n 9) 75.

analysis will focus on deterrence, which is currently a more prominent method of prevention in addition to being all encompassing, as it has an impact on offenders as well as the general public. To a much lesser scale, the methods of incapacitation (rendering the commitment of further crimes impossible for someone, i.e. through incarceration) and reform/rehabilitation (based on the moral education and social reintegration of the offenders) will also be discussed.

It is, however, argued that deterrence, reform or incapacitation cannot justify punishment as independent rationales, but should be related to the promotion of an ultimate social good, since crime prevention by itself is not a justifiable aim, but is presumed to promote superior goals, such as social betterment and public safety.[17] Initial articulations of this superior aim centred on maximising public happiness,[18] but gradually evolved into the notion of maximising social well-being.[19] Relating crime prevention to the utilitarian aim of public well-being usually introduces some limitations to criminal sanctioning. This limitation is realised through introducing certain considerations in the sanctioning rationale such as proportionality and respect for personal dignity, which are related to achieving communal well-being.[20] These principles are considered important for overall social good and, therefore, disregarding them could ultimately generate disutilitarian results, even if, in short-term, an individual result seems utilitarian.[21] Consequently, the need for specifying the ultimate good and its constitutive elements and for subordinating crime prevention to serving this goal, weakens the presumption that maximising crime prevention could justify any measure, which could eventually result in

[17] Michael Philips, 'The Justification of Punishment and the Justification of Political Authority' (1986) 5 Law and Philosophy 393, 395.

[18] Honderich (n 9) 87.

[19] Ibid.

[20] Andrew Ashworth and Elaine Player, 'Sentencing, Equal Treatment and the Impact of Sanctions' in Andrew Ashworth and Martin Wasik (eds), *Fundamentals of Sentencing Theory* (Clarendon Press, Oxford 1998) 253; Herbert L.A. Hart, *Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford University Press, Oxford 1968) 11-2; However Hart argues that individual cases might be treated on a purely consequentialist basis, if the benefits are so substantial, as to outweigh concerns of injustice; Honderich (n 9) 91-2, 95-8.

[21] This is a 'rule-utilitarianism' rationale, which decides upon the utility of certain behaviours once they are generalised as a phenomenon based on certain moral rules, as opposed to rule utilitarianism, which assesses utility on a case by case basis. It would appear that, especially for state policies that require consistency, a more rule-utilitarian approach should be adopted. See Kent Greenawalt, *Conflcts of Law and Morality* (Oxford University Press, New York 1989) 96-7.

generalising excessive responses, unjust victimisations and ultimately, social disutility.[22] Punishing criminals might initially appear utilitarian, but, as will be argued here, there are certain forms of law-breaking, where hard punishments for deterrence, incapacitation or reform might not fulfil this goal.

According to Strong, the above considerations have shaped three utilitarian punishment principles:

> 1. Punishment should serve the end of promoting the common good;
> 2. Punishment is justified, if, more than other alternatives in dealing with antisocial behaviour, it serves as a needed and effective means of maximizing good or minimizing future evil;
> 3. When there is neither production of good future consequences, nor prevention of bad ones to be had from punishing an offender against the law, punishment should not be inflicted.[23]

If these requirements are not fulfilled by the chosen punishment, the utilitarian should find the penalties unjustifiable and seek more efficient and less harmful ones.[24] Let us begin by discussing the dominant function of deterrence.

2.2 Preventive functions and ECD

2.2.1 Basic notions of deterrence

Deterrence relates either to offenders (special) or the public (general). Special deterrence attempts to prevent recidivism by imposing a serious hardship on the offender by sanctioning him/her to discourage re-offending for fear of similar or increased penalties. General deterrence is facilitated by inducing fear of punishment in the public, which, being made aware of the harm imposed on the offender, will remain law-abiding in order to avoid a similar fate. Deterrence relates strongly to the actual possibility of a designated penalty being imposed, rather than solely on the existence of the provision dictating the imposition

[22] Anthony Duff, *Punishment, Communication, and Community* (Oxford University Press, Oxford 2001) 8.
[23] Strong (n 16) 189.
[24] ibid; Honderich (n 9) 88.

of sanctions, since the deterring effect also depends on the actual capacity of the authorities to impose the penalties designated.[25] If the actual possibility of punishment is low, based on a lack of enforcement of the existing sanctions, the deterrent effect will inevitably be weaker. In fact, research has established that increased penalties will not usually improve the levels of deterrence.[26]

There is also an additional function of general deterrence, which entails the capacity of punishment to cultivate normative inhibitions against law-breaking and, in that sense, to morally educate citizens to respect the law.[27] The fact that certain behaviour is declared and proven to be punishable gradually solidifies a social aversion towards it, which is subsequently transformed into the habitual avoidance of similar acts.[28] Robinson names this function the 'normative crime control mechanism'.[29] Finally, general deterrence can also partially function through differentiating punishment between acts of different harmfulness in order to induce people to opt for less serious offences.[30] We will now proceed to assess how different degrees of punishment could operate in relation to deterring ECD protesters.

2.2.2 Extent of punishment and efficient deterrence of ECD

If we are to argue for lenient or high punishment in relation to the deterrent effect of cybercrime laws, we would first have to take into account the practical difficulties of assessing the efficiency of prevention in the first place, since, as seen above, deterrence relies more on the certainty of a penalty rather than its extent.[31] Enforcement problems are relevant to cyberdeviancy, due to the international nature of these protests. As Brenner argues, 'As currently configured, the law enforcement model cannot create a credible

[25] Androulakis (n 7) 41-2; Robinson, 'Why Does the Criminal Law Care What the Layperson Thinks Is Just?' (n 14) 1845-6.

[26] William Young, 'The Effects of Imprisonment on Offending: A Judge's Perspective' (2010) 1 Criminal law Review 3, 17.

[27] Chris M.V. Clarkson, Heather M. Keating and Sally R. Cunningham, *Criminal Law: Text and Materials* (7th edn Thomson Reuters Ltd, London 2010) 34.

[28] Androulakis (n 7) 43; Hyman Gross, *A Theory of Criminal Justice* (Oxford University Press, Oxford 1979) 400-1.

[29] Robinson, 'Why Does the Criminal Law Care What the Layperson Thinks Is Just?' (n 14) 1840.

[30] Honderich (n 9) 83.

[31] See (n 25).

threat of apprehension and punishment for cybercriminals.'[32] For hacktivists, however, their past norms of openness and identifiability, at least, meant that enforcement would be much easier, as acts like virtual sit-ins often were and, still, are traceable to their perpetrators. After all, deterrence is far more reliant on the potential for enforcing the sanctions, which in the case of hacktivists could be more likely, than the imposition of very strict, high penalties that are uncertain.[33] The ease of traceability of online protesters, thus, challenges the rationale that the difficulty in apprehending and punishing cybercriminals would justify increasing sanctions as a counterbalancing factor to the weak enforcement capabilities.

Moreover, assessing the degree of punishment necessary to achieve effective deterrence becomes difficult due to the protesters' differing mentalities, in addition to the lack of proof of any consistent deterrent effect of serious penalties, such as long-term incarceration.[34] First, there is the case of casual participants. In acts, such as virtual sit-ins, which require mass participation and are often publicised in advance, most of the participants will be everyday users that casually join protests in relation to specific causes they deem just. Arguably, for the majority of protesters, the publicisation of only a few prosecutions would be adequately discouraging.[35] Generally, law-abiding citizens would be deterred, even by the threat of low penalties, such as fines or a few days of imprisonment, since they will often lack the determination and political conviction, which could render them defiant of even a potential legal risk.[36] Moreover, the usually altruistic, non-profit nature of hacktivism means that the benefits for the protesters would often be too uncertain, prospective or indirect to outweigh a prosecution risk. In addition, the risk of facing actual punishment would be more salient for easily traceable hacktivists than for anonymous deviants, since the traceability of hacktivists would make the actual imposition of the penalty more likely. Therefore, the state need not resort to lengthy imprisonment

[32] ibid 208.

[33] Androulakis (n 7) 41-2; Robinson, 'Why Does the Criminal Law Care What the Layperson Thinks Is Just?' (n 14) 1845-6.

[34] Alan Norrie, *Crime, Reason and History: A Critical Introduction to Criminal Law* (Butterworths Tolley, London 2001) 203-4.

[35] Stephen Mansfield-Devine, 'Anonymous: Serious Threat or Mere Annoyance?' (2011) 1 Network Security 4, 7.

[36] For example, the threat of being under surveillance and having repercussions on university Internet access proved adequate to deter participants from realising the protest. Jill Lane and Ricardo Dominguez, 'Digital Zapatistas' (2003) 47 TDR 129.

penalties to efficiently deter casual protesters, but just demonstrate a level of adequate interest and efficiency in imposing milder penalties in order to deter most Internet users from participating.

For the more determined participants/organisers, it is argued that in order to overwhelm their strong political convictions and their potential will to accept potential punishment, deterrence could probably be achieved only with substantially high penalties.[37] Additionally, it has been argued that incarcerating the civil disobeyer who has violated a statute is not likely to deter others similarly motivated, unless the sentence is oppressive.[38] However, it would appear that even for organisers that could be deterred, just the prospect of prosecutions could be enough to deter these protesters. Organiser-hacktivists of the earlier eras, for example, had only resorted to these types of protests under the presumption that their activities would not be prosecuted as criminal.[39]Then, when the threat of sanctions became too serious and more probable, even devoted organisers such as the members of EDT or the Electrohippies decided to abstain from protests in order to avoid any probable prosecution.[40]

Severe punishment of organising members, however, could be considered effective as an example to ensure general deterrence. Despite the fact that general deterrence could

[37] Kimberley Brownlee, 'Civil Disobedience' (*Stanford Encyclopedia of Philosophy*, 23 December 2009) <http://www.illc.uva.nl/~seop/entries/civil-disobedience/> accessed 12 August 2011; For example, the government might conclude that the vigour of opposition to an unpopular war requires severe penalties to deter illegal protest. Columbia Law Review Association, 'Sentencing in Cases of Civil Disobedience' (1968) 68 Columbia Law Review 1508, 1512. In the case of Weatherhead in the UK, he was the only one of four accused that was an organiser of events and who declined to plead guilty, preferring to face the full penalty instead. Brid-Aine Parnell, 'Brit Mastermind of Anonymous Paypal Attack Gets 18 Months' Porridge' (*The Register*, 24 January 2013) <http://www.theregister.co.uk/2013/01/24/uk_anonymous_hackers_sentencing_payback/> accessed 26 January 2013.

[38] Columbia Law Review Association (n 37) 1535-6.

[39] Evan R. Goldstein, 'Digitally Incorrect' (*The Chronicle Review*, 03 October 2010) <http://chronicle.com/article/Digitally-Incorrect/124649/> accessed 12 August 2011; Bret Stalbaum, 'Why I Made a Formal Statement to the UCSD Police' (*Walking Tools,* 21 July 2010) <http://www.walkingtools.net/?p=489> accessed 26 October 2010; The Electrohippies Collective, 'Cyberlaw UK: Civil Rights and Protest on the Internet' (*iwar.org,* 2000)<http://www.iwar.org.uk/hackers/resources/electrohippies-collective/comm-2000-12.pdf> accessed 15 February 2013.

[40] Ricardo Dominguez of EDT and the Electrohippies are typical examples of hacktivists that abandoned their hacktivist, virtual sit-in organising, when they were faced with potential prosecutions. Ricardo Dominguez, 'FBI Has Ended the "Investigation" of Vr Sit-in Performance' (*b.a.n.g.,* 12 November 2010) <http://bang.calit2.net/2010/11/fbi-has-ended-the-“investigation”-of-vr-sit-in-performance/> accessed 20/05/2011; The Electrohippies Collective (n 39).

dictate exemplary penalties in order to discourage the public from participating in hacktions, such decisions have generated much controversy, as they often appear to undermine notions of individual right and responsibility.[41] Even if stricter punitive policies prevail, it is questionable whether there is a need for very harsh penalties in order to deter the general public, since, as seen above,[42] the majority of protesters or potential protesters, would be easily deterred anyway. Therefore, even lenient penalties for core protesters would have an adequately generally deterrent effect.

Moreover, oppressive punishments is usually considered only when prevention would be more important, such as when the offence demonstrates a high degree of risk to citizens' physical integrity and a high degree of frequency.[43] As was discussed in chapter two,[44] ECD usually does not fulfil such criteria of dangerousness, severity and persistence and, therefore, exemplary punishment would under normal circumstances be an exaggerated response, even if increased penalties had a guaranteed deterrent effect, which has been considered doubtful.[45] Naturally, for hacktivist actions that disregard moral standards, such as non-harmfulness, higher penalties could be a possibility, but again dangerousness, persistence and influence of the punishment on general public ought to be taken into account before making examples out of specific protesters.

However, apart from being generally excessive, severe, exemplary penalties could prove inefficient in preventing hacktivists, since for hardcore protesters, the extent of punishment might not even feature in the protesters' decisions, instead being considered indicative of state authoritarianism.[46] Strongly idealist activists could be analogised to 'free radicals', who are usually untouched by the threat of liability and punishment.[47] The same goes for

[41] Norrie (n 34) 207. For example, the 4 year imprisonment penalty for posting riot-inciting comments on Facebook as an exemplary punishment for using social media to incite and organise riots has caused much controversy in relation to the utility of such measures. Julian Baggini, 'England Riots: Are Harsh Sentences for Offenders Justified?' (*The Guardian*, 17 August 2011) <http://www.guardian.co.uk/uk/2011/aug/17/england-riots-harsh-sentences-justified> accessed 08 September 2011.

[42] See Part 2.2.2 Extent of punishment and efficient deterrence of ECD.

[43] Andrew von Hirsch, 'Censure and Sanctions' (Oxford University Press, Oxford 2003) 50.

[44] See Ch 2, Part 3.2 Non-violence.

[45] See (n 26).

[46] Martin C. Loesch, 'Motive Testimony and a Civil Disobedience Justification' (1990) 5 Notre Dame Journal of Law, Ethics & Public Policy 1069, 1103; Gregor Allan, 'Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative' (2005) New Zealand Law Review 149*,* 166-7.

[47] Meiring De Villiers, 'Distributed Denial of Service: Law, Technology & Policy' (2007) University of New South Wales Faculty of Law Research Series, Paper 7, 1, 6.

many hackers, who are not hindered easily by the legal costs, when a technical challenge presents itself or a problem that relates to the wider community arises.[48] The intensity of political convictions that characterise hardcore hacktivists, in conjunction with the anti-authoritarian mentality of many of those protesters that also come from a hacker background,[49] could render insignificant the basis for effective deterrence - the balance of cost/benefits - since protesters will lack this individualistic, calculative mentality and will be more self-sacrificial.[50] This would render serious or harsh punishment irrelevant and inefficient in providing the desired preventive results, thus, being unjustifiable even without examining its ultimate utility.

Moreover, the preventive potential of high penalties could be compromised by the fact that harsh penalties could propagate more numerous and radical protests. According to Sherman, ‘sanctions provoke future defiance of the law (persistence, more frequent or more serious violations) to the extent that offenders experience sanctioning conduct as illegitimate, maintain weak bonds to the sanctioning agent and community and deny their shame and become proud of their isolation from the sanctioning community.’[51] The portrayal of the legal system and the cybercriminal justice regime as intolerant and harsh, could, therefore, satisfy the criteria mentioned by Sherman and lead to more and more radical protests.

The recent, more damaging and radical activities of Anonymous demonstrate such a tendency, partly at least, as a response to stricter persecution of political activities online and arrests and convictions of their peers, both online and offline.[52] Consequently, the

[48] Reid Skibell, 'Cybercrime and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act' (2003) 18 Berkeley Technogy Law Journal 909*,* 936-7.

[49] Anti-authoritarianism is a basic premise of the hacker ethic. See Ch 1, Part 1.5 The role of hacktivists as hacker/political entities of counterpower.

[50] As research has shown, individuals that have adopted the hacker ethos would fail to abide by the cost-benefit expectations of the criminal justice system. Allan (n 46) 166.

[51] Lawrence W. Sherman, 'Defiance, Deterrence, and Irrelevance: A Theory of the Criminal Sanction' (1993) 30 Journal of Research in Crime and Delinquency 445*,* 448-9.

[52] Data thefts and exposure of information online were the response to dissident crack-downs by the police during offline protests of the Occupy movement in the US. Elinor Mills, 'Anonymous Exposes Info of Alleged Pepper Spray Cop' (*CNet,* 26 September 2011) <http://news.cnet.com/8301-27080_3-20111813-245/anonymous-exposes-info-of-alleged-pepper-spray-cop/> accessed 15 August 2012; Anonymous even took down the US department of Justice website to protest the crack-down on the major filesharing website megaupload and its owner. Laurie Segall, 'Anonymous Strikes Back after Feds Shut Down Piracy Hub Megaupload' (*CNN Money,* 20 January 2012)

imposition of strict penalties, despite aiming at increasing the deterrent effect of punishment, could instead feed a phenomenon of ‘cumulative extremism’,[53] thus, creating a vicious circle of radicalisation on the part both of the hacktivists and the authorities.[54] It is therefore questionable whether harsh punishments should be considered adequately deterrent or more deterrent than more lenient penalties, which seem to have similar deterrent potential in most cases where protesters could be deterred. Moreover, as has been discussed, the threat or actual imposition of high penalties has resulted in less harmful protests to subside, yet more radical and harmful protests have multiplied as a response, thus proving counterproductive in terms of crime prevention. Even if we consider harsh penalties more deterrent than lenient penalties - a tenuous conclusion, from what has been discussed - the ultimate utility of harsh penalties, as will be seen in the next section, is also doubtful.

2.2.3 Are highly punitive sanctions for ECD utilitarian?

It is now time to assess whether, even if we accept that there is increased preventive potential in high penalties, these would also promote overall social well-being. Utilitarians punish serious offences more strictly because they see a need for society to more actively prevent increasingly harmful offences, presuming that stricter punishments would normally have more preventive results and, consequently, promote social well-being by reducing overall crime.[55] However, as Brody has found: ‘there is no evidence that longer custodial sentences produce better results than shorter sentences’[56] a point already noted above.[57] Suggestions for harsher punishments will thus initially be tempered by the fact that crime prevention is always an uncertain, future possibility, whereas the harms caused by the imposition of punishment are immediate and certain.[58]In cases where ECD protesters make efforts to abide by the moral criteria mentioned in Chapter Two, harmfulness is usually kept

<http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm> accessed 20 July 2013.

[53] Roger Eatwell, 'Community Cohesion and Cumulative Extremism in Contemporary Britain' (2006) 77 The Political Quarterly 204.

[54] Sherman (n 51).

[55] Strong (n 16) 189-90.

[56] Sthephen R. Brody, *The Effectiveness of Sentencing: A Review of the Literature (*Home Office Research Study No.35, Home Office Research Unit, London 1976) 39.

[57] Part 2.2.1 Basic notions of deterrence.

[58] Barbara Hudson, *Justice in the Risk Society: Challenging and Re-Affirming Justice in Late Modernity* (Sage Publications Ltd, London 2003) 24.

low, since protesters attempt to minimise any potential damage and do not impair the full functionality of state agencies' or companies' websites.[59] Instead, protesters try to facilitate an easier and less costly recovery and can even allow time for countermeasures in cases of pre-publicised protests.[60] Consequently, for moral, less dangerous protesters, the strong need of prevention will be lacking, even if harsh penalties are considered efficient. High penalties could thus, prove excessively harmful in relation the potential harms of the protesters. Naturally, for protests that result in high damages or are done for non-political reasons, their claim for reduced punishment could be weakened accordingly, since the potential harms they might inflict, will be so high as to potentially balance the harm of the high punishment inflicted. Therefore, if one relates the degree of damage to utilitarian conceptions of dangerousness and harm, less harmful forms of ECD would offer less justification for serious preventive measures for avoiding undue harms.[61]

However, if we consider that an additional aspect of utility is general deterrence, even disproportionate punishment of certain activists could be deemed utilitarian by preventing violations of law on a presumably larger scale through public intimidation.[62] Especially in systems suffering from weak enforceability, such as cybercriminal law,[63] increased punishment for those actually apprehended could, arguably, counter the inefficiency of the system.[64] Even though such rationales for punishment could be and are, in fact, promoted on the bases of political ends,[65] the question to be asked here as well is whether there is an inherent utility in generally preventing activities like ECD and whether such goals, as demonstrating the state's firmness in hindering such activities in general and preserving the rule of law and democratic order through serious punishment would be ultimately served.

A realisation of the potential positive elements of ECD, such as political engagement and the increase of democratic deliberation globally, for example, could cause a reconsideration of the utility of generally and absolutely deterring these activities and condemning their perpetrators to long-term imprisonment that can prove excessively harmful to them and

[59] Mansfield-Devine (n 35) 8.
[60] Stalbaum (n 39) The most typical example is the Lufthansa protests in Germany, where protesters even notified the authorities and gave Lufthansa time to prepare. Ricardo Dominguez, 'Electronic Disobedience Post-9/11' (2008) 22/5 Third Text 661.
[61] Hart, *Punishment and Responsibility* (n 20) 163.
[62] Norrie (n 34) 206.
[63] See above and also Ch 4, Part 3.4 Resources, information and lack of harmonisation**.**
[64] Andrew Ashworth, *Sentencing and Penal Policy* (Weidenfeld and Nicolson, London 1983) 339.
[65] Norrie (n 34) 207; See also Facebook example in (n 41).

their families.[66] This is because protesters, who express their dissent according to the moral standards described in the previous chapter, will often lack the fully malign and anti-social character justifying stricter criminal punishments that defy the social good, while these online protests might also operate as a social tension - release valve, substituting for more radical and damaging offline activities.[67] Moreover, the increased penalties that compensate for weaker enforceability could be inconsistent with the easier traceability and prosecutability of hacktivists. Consequently, the designated high penalties meant to compensate for low enforceability in the cybercrime regime would often prove excessively harmful in dealing with minor deviants that are also generally more easily traceable and prosecutable. Moreover, harsh penalties could also prove disutilitarian by alienating politically considerate citizens, who will feel excessively harmed by harsh sanctions, in addition to being victimised by the injustices protested against.[68]

Instead of affirming the state's vigour in maintaining order and making citizens more obedient, punitive policies against socially considerate and non-dangerous protesters could harm the legitimacy of the current regime and alienate more citizens, since attempts that appear to restrict free political expression have often led to the intensification of political reactions and to a rising moral anger towards the authorities.[69] According to Dworkin, the

[66] Prosecuted protesters on multiple felonious charges have lost their jobs or have been unable to find one while awaiting trial, even threatening to commit suicide. Gerry Smith and Ryan J. Reilly, 'Alleged 'Paypal 14' Hackers Seek Deal to Stay out of Prison after Nearly 2 Years in Limbo' (*Huffington Post*, 18 May 2013) <http://www.huffingtonpost.com/2013/05/18/paypal-14-hackers_n_3281768.html> accessed 20 May 2013; See discussion about Aaron Swartz in Lawrence Lessig 'Prosecutor as Bully' (*Lessig Blog, v2*, 12 January 2013) <http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully> accessed 20 June 2013; Zoe Lofgren and Ron Wyden 'Introducing Aaron's Law, a Desperately needed Reform of the Computer Fraud and Abuse Act' (*Wired,* 20 June 2013) http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/ accessed 21 June 2013.

[67] See Ch 2, Part 3.5 Last resort.

[68] Greenawalt (n 21) 275; Craig P. Colby, 'Civil Disobedience: A Case for Separate Treatment' (1968) 14 Wayne Law Review 1165, 1167-8; Bob Garfield, 'Defending Hacktivism' (transcript of Interview with Evgeny Morozov, *On the Media*, 17 December 2010) <http://www.onthemedia.org/transcripts/2010/12/17/02> accessed 20 May 2011.

[69] Kent Greenawalt, 'A Contextual Approach to Disobedience' (1970) 70 Columbia Law Review 48, 79. An example of how state laws and prosecutors' actions could be considered excessive and generate a general uproar in relation to overpunishing online political lawbreaking is the case of Aaron Swartz. Swartz was very aggressively persecuted by the authorities that he eventually committed suicide before the threat of potentially facing exorbitant penalties for his illegal online activism. This event led to many protests both offline and online and to a general outcry against the punitive criminal justice system in the US. Anonymous expressed their support by defacing the website of the US Sentencing Commission, whereas cyberlaw theorists, such as Lessig, emphasised the need for more

way for maintaining respect for the rule of law is through respecting citizens' liberties and rights, and not through harshness.[70] Harsh punishments and the partly ensuing radicalisation of protesters would, thus, be non-utilitarian as well, since the increases in protests would corrupt hacktivist practices, leading protesters to become more damaging and go underground to avoid the potentially high penalties. Of course the pervasive and increasingly radical protests ensuing from the perceived lack of legitimacy of those punishments would also lead to more security breaches overall, thus impacting on overall cybersecurity.

Moreover, high punishments of moral protesters could also generate sympathy towards hacktivists on behalf of the public and portray the state as oppressive, thus, further impacting on the perceived legitimacy of the regime.[71] As Reed argues, for cyberspace laws to be followed, they need to command the respect of the online community by being in accordance with established cyberspace norms or, at least, appear meaningful to users.[72] Research conclusions, as I will discuss below, indirectly demonstrate how a large part of the public would find the harsh cybercrime penalties inconsistent with user norms and their perceptions of hacktivist actions and appropriate levels of punishment. For example, Yar argues that, according to research, hacking has often been seen positively, especially by the younger generations as an act of resistance, in addition to other qualities as well, such as technological virtuosity, despite it being explicitly considered criminal.[73] More specifically, although the research was conducted almost 15 years ago and refers to hacking more generally without including the factor of moral political, expressive motives, almost 30% of the respondents argued that hacking was acceptable, while almost half of the respondents declined to consider hacking as theft.[74] Moreover, the majority of respondents also seemed to adopt lenient attitudes in relation to the nature and severity of the punishment to be imposed on hackers.[75]Further research also found great public acceptance of the

considerate responses from the prosecutors. Lawrence Lessig, 'Prosecutor as Bully' (*Lessig's Blog v2,* 12 January 2013) <http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully> accessed 15 February 2013.

[70] Dworkin (n 4) 205-7.

[71] Strong (n 16) 190.

[72] Chris Reed, *Making Laws for Cyberspace* (Oxford University Press, Oxford 2012) 20, 23.

[73] Majid Yar, 'Public Perceptions and Public Opinion About Internet Crime' in Yvonne Jewkes and Majid Yar (eds), *Handbook of Internet Crime* (Willand Publishing, Devon 2010) 104-119, 106.

[74] Paul Dowland et al., 'Computer Crime and Abuse: A Survey of Public Attitudes and Awareness' (1999) 18 Computers & Security 715, 720.

[75] ibid.

youthfulness of law-breaking protesters and of the spontaneity of the acts as mitigating factors,[76] thus, also supporting mitigated penalties, at least for a part of protesters, who are young or might have acted due to spontaneous urge to join in with the rest of the iRC group.[77] Despite the established view that the public is of a punitive disposition, this apparent punitiveness is based on the lack of knowledge of the potential alternatives to imprisonment.[78] Researchers have found that, when the public is actually informed of specific cases of criminality and of alternative, more lenient and less costly forms of punishment than custodial sentences, many tend to prefer more lenient penalties and methods of punishment than those handed down by courts for similar incidents.[79] As it is argued, 'surveys that include questions that assess diverse ideological views on correctional policies find that public opinion is complex, progressive and under certain conditions, not unyieldingly punitive.'[80] Consequently, the more the public becomes familiar with alternative punishments and hacktivist tactics, in addition to their moral motives, strict custodial punishments would appear illegitimate for a larger part of the general public, thus further weakening the claim of the state to citizens' obedience.

Apart from the obvious disutility of having more numerous and less moral attacks on computer networks created by those considering high penalties as illegitimate, radicalisation of protesters would even have an impact on the quality of online politics more generally, since socially considerate protesters would potentially refrain from resorting to more radical protests, considering them immoral and inefficient. Fear of excessive sanctions[81] and their moral beliefs would lead the more moral protesters to refrain from actively participating in the cyberpolitical arena, a trend which could gradually lead to the moral deterioration of political discourse, leaving the punitive state and the

[76] Julian V. Roberts and Mike Hough, 'Sentencing Riot-Related Offending: Where Do the Public Stand?' (2013) 53 British Journal of Criminology 1, 8-9.

[77] See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism. Most of the protesters prosecuted for the Paypal protests in the UK were in their teens or 20s. Parnell (n 37).

[78] Mike Hough and Julian V. Roberts, 'Sentencing Trends in Britain: Public Knowledge and Public Opinion' (1999) 1 Punishment & Society 11, 12, 15-8, 21; Francis Cullen, Bonnie Fisher and Brandon Applegate, 'Public Opinion About Punishment and Corrections' (2000) 27 Crime and Justice 1, 4-5; Roberts and Hough (n 76) 5.

[79] Cullen, Fisher and Applegate (n 78) 7-8; Roberts and Hough (n 76) 10-3, 16-7; Hough and Roberts (n 78) 17-8.

[80] Cullen, Fisher and Applegate (n 78) 8.

[81] James Ball, 'By Criminalising Online Dissent We Put Democracy in Peril' (*The Guardian,* 01 August 2011) <http://www.guardian.co.uk/commentisfree/2011/aug/01/online-dissent-democracy-hacking> accessed 21 September 2011.

radicalised protesters to clash in non-productive, mutually retaliatory conflicts.[82] Condemnation of protesters as dangerous cybercriminals would also delegitimise their causes and allow the state to avoid addressing these causes of protest as indeed serious.[83] Consequently, serious punishment that eliminates activities with the potential to challenge informational monopolies would further limit the chances of contesting important social injustices, ultimately eliminating processes like CD that, as Habermas argues, guarantee the legitimacy of the state.[84]

Alternatively, milder and alternative types of sanctioning ECD could increase personal autonomy and promote conscientious political activity with more faith in the justness of the legal system. Simultaneously, lenient penalties would consolidate an understanding of the injustices of the current socio-political system with the need to maintain respect for law. This would be expressed in the demonstration of a social understanding of the existence of potential reasons for dissent through lenient responses to it, but also induce a respect on behalf of the protesters for the legal system according to the morality and dangerousness of their tactical choices.

Apart from avoiding undue over-punishment of protesters, the imposition of equally efficient, yet more lenient, penalties would not immediately render punishment illegitimate in the eyes of protesters and could induce a moral reconsideration of their tactical choices, thus, leading more protesters to rationally reconsider their tactical approaches.[85] This could be inferred from the first years of hacktivist activity, where crack-downs on hacktivists were not as aggressive and the threat of lower than current penalties was not so salient, resulting in hacktivist actions following the ethical standards, discussed above, more

[82] The example of the first more principled hacktivist groups gradually leaving the scene to the more chaotic and less principled collectives, such as Anonymous, many parts of which consider the moral dictates of the former groups, such as identifiability, restrictive and risky, is typical of how punitive measures have gradually also led to the departure of these moral groups from the fore of the online political scene.

[83] Zizek has supported this rationale even for not strictly ideological, violent outbursts, such as the London riots of 2011, the condemnation of which, results in bypassing the actual reasons that led to these riots. Slavoj Zizek 'Shoplifters of the World Unite' (*London Review of Books*, 19 August 2011) <http://www.lrb.co.uk/2011/08/19/slavoj-zizek/shoplifters-of-the-world-unite> accessed 24 August 2011.

[84] See Ch 2, Part 2.2.4 Conclusion.

[85] Hart (n 20) 163; Colby (n 68) 1167; The nature of the targeted website plays an important role since governmental websites might be considered to be providing important services (administration of justice, crime prevention) and thus attacking them could incur high penalties. For private websites, if it is a commercial website, the losses incurred from being unable to offer services during the protest could also raise the potential penalties.

diligently.[86] A potential legal risk that would not be too exhausting, but would demand a certain sacrifice from the dissidents, could, thus, avoid radicalising protesters against the state and could, instead, lead to political maturation of ECD protesters and differentiate ECD from superficial symbolic online politics or hacking pranks.[87] As Morozov has argued, political causes and groups attain significant substance and purpose, when participation and action requires a certain degree of sacrifice from them.[88]

Furthermore, on a more practical basis, more lenient approaches would assist in alleviating the over-burdened criminal justice system, both in terms of time and resources, but also in terms of decongesting crowded detention facilities; a situation that would worsen by imprisoning hacktivists. Such decisions should definitely play a role in the courts deciding on the utility of incarcerating low-level criminals like hacktivists, since prison overcrowding has become an important social problem in many jurisdictions.[89] Finally, leniency would prevent the potential corruption of non-criminally-minded citizens through forcing them to interact with purely criminal convicts if incarcerated[90] and avoid the stigmatisation and the reduced social opportunities flowing from having a criminal record, while also reducing the important, collateral social damage to the families and communities of the offenders, thus, avoiding further disutilitarian consequences.[91] It would appear

[86] Ch 1, Part 2.2.1 The first era of hacktivism and the birth of electronic civil disobedience.

[87] Henrik S. Christensen, 'Political Activities on the Internet: Slacktivism or Political Participation by Other Means?' (2011) 16 First Monday <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3336/2767> accessed 17 December 2012.

[88] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs, New York 2011) 189.

[89] See for example how prisons are overcrowded in the UK and main reasons for that is lack of alternative penalties to imprisonment and punitive policies towards non-dangerous offenders. Criminal Justice Alliance,'Crowded Out: The Impact of Prison Overcrowding on Rehabilitation' (*The Criminal Justice Alliance,* 2012) <http://www.criminaljusticealliance.org/Crowded_Out_CriminalJusticeAlliance.pdf> accessed 20 June 2013; Morag MacDonald, Robert Greifinger and David Kane, 'The Impact of Overcrowding' (2012) 8 International Journal of Prisoner Health; For US problem of overcrowding and suggestions for more moderate responses to crime see: Karina Kendrick, 'The Tipping Point: Prison Overcrowding Nationally, in West Virginia, and Recommendations for Reform' (2011) 113 West Virginia Law Review 585.

[90] Michael A. Wolff, 'Evidence-Based Judicial Discretion: Promoting Public Safety through State Sentencing Reform' (2008) 83 New York University Law Review 1389*,* 1395.

[91] Some of the problems are marginalisation and increase of unemployment, dissolution of family bonds and consequently, reliant social bonds, increased fear of crime, etc. see: Council on Crime and Justice, *The Collateral Effects of Incarceration on Fathers, Families, and Communities* (Research Demonstration Advocacy, 2006)< http://www.racialdisparity.org/files/CEI%20FINAL%2003312006.pdf> accessed 15 February 2013, 4-7.

therefore that deterrence through high custodial sanctions could have less preventive and generally more socially harmful consequences than more lenient approaches in the case of moral hacktivists. Before concluding the discussion on utilitarian prevention, though, the incapacitation and reform/rehabilitation functions of punishment in relation to prevention will also be discussed.

2.2.4 The utility of incapacitating and reforming hacktivists

Incapacitation is another function of punishment for preventing crime. However, incapacitation relates only to direct prevention of offenders from re-offending and could not constitute a general rationale for punishment. Incapacitation traditionally relates to lengthy custodial sanctions that prevent offenders from causing similar social harms as those that lead to their punishment, usually by incarcerating or generally restricting their freedoms for a period of time so as to make sure that they do not have the chance to reoffend; at least beyond the strict confines of their prison. In the case of hacktivism incapacitation could, indeed, be achieved through long term incarceration. However, imposing even lengthier custodial sentences on hacktivists that would operate, not just as a deterrent, but as a more permanent incapacitating tactic, would generate similar problems, such as those discussed for deterrence and lengthy custodial sentences above. Since incapacitation is usually a method considered for very dangerous offenders, it would be very questionable whether incapacitative rationales could justify long-term incarceration for hacktivists, when they lack this element of dangerousness.

The use of imprisonment is also questionable as an incapacitative method, when there are far more lenient preventive methods for non-dangerous offenders, such as supervised release, and restrictions on Internet use that are not considered as harmful for offenders, such as electronic tagging or a restriction on the use of Internet devices.[92] More particularly, since the offences in question relate to online activities, incapacitation could be achieved with penalties such as imposing restrictions on the Internet use of convicted protesters, which could act preventively in relation to their participation in similar offending activities. The level of effectiveness is not the same, of course, once the offender is not as physically restricted and means for bypassing the Internet-related restrictions

[92] See also Ch 5, Part 2.5 Technology-based penalties.

could be found much more easily. However, Internet-restrictive measures could also prove efficient due to their specialised form in relation to the nature of hacktivist offences and would also avoid causing the collateral harms to offenders that are inevitable consequences of totally restricting their freedoms by incarcerating them, thus allowing them to find work more easily and be with their families.[93] Even though such processes might entail costs of monitoring, new technologies have made surveillance easier,[94] with relevant technologies constantly becoming more efficient and accurate, thus allowing authorities to impose restrictions on Internet use that would be harder to bypass.

Consequently, the crucial question for incapacitation is whether potentially violable measures of incapacitation would be preferable to more radical measures such as incarceration. A more general question to be asked here, however, is whether hacktivists would be citizens that the state would have an interest in incapacitating on a more general scale by harsh imprisonment penalties. Given their low level of dangerousness, most protesters, especially those attempting to employ the discussed moral criteria that relate to CD or plain casual participants, would normally be socio-politically considerate citizens that the state would not generally have an interest in preventing their interaction with other members of the society. Therefore, even under an incapacitation scope, serious imprisonment penalties could be considered disproportionately harmful in achieving the desired prevention compared to the dangerousness of the offenders and to existing, more lenient alternatives, while they would also have disutilitarian indirect social effects to hacktivists, their kin and the state.[95]

[93] Supervised Internet use has been used extensively as a precautionary bail term and as a penalty in cases of cybercriminality. See Gabriel Gillett, 'A World without Internet: A New Framework for Analyzing a Supervised Release Condition That Restricts Computer and Internet Access' (2010) 79 Fordham Law Review 217.

[94] Tagging as a bail condition for imposing curfew has been approved by the UK Home Office as a legitimate policy. Home Office, 'Electronic Monitoring on Bail for Adults - Procedures' (Home Office Circular 25, London, 2006) Internet use monitoring software is also becoming more specialised and could be combined with more traditional technologies in order to facilitate the monitoring of Internet use. BBC, 'Email and Web Use 'to Be Monitored' under New Laws' (*BBC,* 01 April 2012) <http://www.bbc.co.uk/news/uk-politics-17576745> accessed 15 April 2012; Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London 2011) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf accessed 03 August 2013, 30.

[95] For example, electronic tagging has been considered a more economic means of sanctioning than imprisonment. See Adrian Furnham, Alastair McClelland, and Edward D. Baxter, 'The Allocation of a Scarce Correctional Resource: Deciding Who Is Eligible for an Electronic Monitoring Program' (2010) 40 Journal of Applied Social Psychology 1605.

Although the preventive tactic of reform/rehabilitation has contemporarily retreated before deterrent, imprisonment sanctions and prison overcrowding,[96] these aims are still considered a legitimate reason for imposing criminal punishment and are also facilitative of crime prevention, again focused just on offenders, lacking a general preventive effect.[97] Reform theories are founded on the cultivation and recognition of moral guilt by the offenders and the realisation of the nature and normative demands of society, which will, thus, help offenders behave non-criminally in the future.[98] Moreover, the rehabilitation processes entail educational programs that seek to improve the capabilities and skills of law-breakers and, thus, expand their re-socialisation opportunities by giving them the tools for coping with life's practical demands and avoiding the temptations of a criminal lifestyle.[99] According to these theories, through punishment the offender understands the ethical implications and harmful consequences of his actions and he is, thus, morally improved and re-socialised through acquiring useful skills for leading a law-abiding life after release.[100]

However, the usefulness of reform/rehabilitation programs in relation to punishing moral hacktivists could be challenged for various reasons. Cases of hackers, criminal or even recreational, have, indeed, been dealt with through rehabilitation programs.[101] However, the socially considerate and moral nature of ECD would generally render moral rehabilitation less useful and efficient in trying to imprint ethical considerations on protesters, who are already breaking the law due to an intense moral belief and motivation to protest through the use of hacking techniques. This differentiation in morality and motivating rationales between protesters and plain criminals in need of moral education will probably render reforming punishments irrelevant, inefficient or superfluous, much like rehabilitation punishments promoting social and practical skills, as many protesters will have regular, law-abiding and productive lives.[102] Especially considering the current

[96] See (n 89).

[97] David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford University Press, Oxford 2001) 8; Criminal Justice Act 2003, Section 1(c)

[98] Hart (n 20) 26.

[99] Duff (n 22) 5.

[100] ibid; Hart (n 20) 26-7.

[101] Gregor Urbas, 'Criminalising Computer Misconduct: Some Legal and Philosophical Concerns' (2006) 14 Asia Pacific Law Review 95, 100-1.

[102] Majid Yar, *Cybercrime and Society* (Sage Publications Ltd, London 2006) 18-9; Loesch (n 46) 1103; For example, Mettenbrink, was young, had no criminal background and was employed, before he got involved in the protests. Mettenbrink's involvement was a one-off protest against the Church of

overcrowding of prisons, the global budget reductions and the privatisation of the prison system, it would be very questionable whether imprisonment sentences would entail any element of moral reform and social rehabilitation.[103]

One could never rule out some participants having less morally justifiable motives and, thus, be in need of some degree of moral reform. However, hacktivism is usually non-opportunistic. Consequently, it would rarely appeal as a tactic to hackers with criminal intentions, who might be in need of re-socialising punishments, since ECD offers minimal, if any, personal gain or gratification, especially in relation to the potential legal risks. The exceptions could be unauthorised intrusions, such as data thefts, defacements and redirects, which could confer upon their perpetrators recognition of their technical skills by peers for their hacking skills. Even this gratification, though, will mostly be restricted to bragging in hacker forums, rather than any seriously immoral behaviour requiring reform through imprisonment, if, of course, deliberate undue harms have not ensued or if the motives of the protest lack any conscientious moral basis. Morally reforming punishment could have a positive effect for hacktivists, if it could induce a reconsideration of immoral tactics employed and a return to tactics that abide more closely by the moral criteria identified in the previous chapter.[104] Even if reform programs are deemed useful in particular cases for inducing the mitigation of immoral, harmful practices, though, the nature of the penalty will be relatively milder and will usually entail participation in educational programs, rather than a strict and lengthy custodial time. Rehabilitation, thus, seems to generally support more specifically targeted and lenient approaches than generalisation of long-term imprisonment and would generally be more consistent with calls for lenient treatment of protesters.

In sum, the utility of potentially deterring or even eliminating ECD through strict incarceration sanctions appears, at least in principle, of questionable preventive efficiency and social utility for reasons ranging from excessive harms caused by such sanctions to a

Scientology. As the ‘We are Legion’ documentary shows, the penalty had a grave impact on his everyday life and his re-socialisation and did not have any reformative effect on him, as he considered it unfair. Brian Knappenberger, 'We Are Legion: The Story of the Hacktivists' (*YouTube,* 19 June 2013) <https://www.youtube.com/watch?v=ELcAEwJdTeQ> accessed 02 August 2013; See also (n 66).

[103] David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford University Press, Oxford 2001) 17-8, 119, 177-9; Jonathan Simon, *Governing through Crime* (Oxford University Press, Oxford 2007) 142-3.

[104] See Ch 2, Part 3. The criteria of justifiability.

potential inconsistency with public perceptions. Instead, less punitive approaches seem to have the potential to be equally effective as a deterrent and also to produce important, positive effects for contemporary democratic society, and to be less burdensome for the offenders and the prison system as well. Similar conclusions relate to incapacitation, which, even if deemed appropriate for hacktivists, can be achieved through more specialised and lenient penalties than long-term incarceration of protesters. Reform penalties could perhaps justify punishment as a form of educating protesters in relation to more morally legitimate practices. However, even if the current system accommodated such approaches, the nature of reform penalties would prima facie be more lenient than traditionally imposed plain imprisonment, and would, thus, be more consistent with demands for lenient and tolerant treatment of protesters, in the rare cases they might be in need of moral education. Moreover, adopting a more lenient approach to punishment facilitates the implementation of more specialised preventive approaches, such as Internet-based restrictions or educational programs that can correspond to the special, fluid characteristics of hacktivism, while allowing more punitive approaches in cases where hacktivists behave with purely criminal motivations and in ways that disregard the moral criteria discussed in the previous chapter.

This section does not aim to argue for the imposition of low penalties and their specification. This will be done in the last chapter more explicitly and will be based on a more complex theoretical background and in relation to the specific regulatory conditions. Although the use of some current examples has been unavoidable in order to substantiate the arguments used, the purpose of the analysis here is to demonstrate that harsh penalties for hacktivists would often be inconsistent with the forward-looking purposes of crime prevention and with the ultimate utilitarian goal of producing more public well-being than social harms and mainly in the forms of public safety. The next section will demonstrate how harsh penalties could also prove unjustifiable in terms of the blameworthiness of offenders based on rationales that advocate for a deserved penalty in relation to the overall fault of hacktivists.

3. Backward-looking theories

3.1 Morality and punishment: Just Deserts

Despite the importance of crime prevention, concerns relating to restoring the imbalance of justice caused by law-breaking act also play a role in the ultimate justification of punishment, since criminal law and deontological concerns have always been interrelated.[105] Backward-looking theories of retribution focus on the immorality of the offence as the reason for punishment, essentially arguing that whoever deliberately breaks the law must pay a penalty proportionate to the crime's gravity in order for justice to be served.[106] In other words, the extent of punishment is determined according to what is justly deserved - 'just deserts'. To assess the exact deservedness, most theories acknowledge the need for additional considerations beyond the deliberate violation of law,[107] with prima facie guilt being just a necessary prerequisite for considering someone eligible for punishment.[108] Therefore, the numerous interpretations of the theoretical bases for just deserts develop the basic argument of guilt, as a reason for punishment, with additional moral considerations in order to avoid a simplistic, dogmatic justification of punishment based solely on law-breaking.[109]

Currently, just desert is considered an additional factor to utilitarian prevention for assessing the justifiability of imposing punishment, essentially limiting the extent of punishment one would employ for preventive purposes and grounding such a moderating assessment on an overall reviewing of harmfulness and moral blameworthiness. A common perspective attributes a secondary role to just deserts, in addition to the general justifying

[105] George P. Fletcher, *Basic Concepts of Criminal Law* (Oxford University Press, New York 1998) 32. The influence of just deserts in criminal law is evident in the US Sentencing guidelines and the justifying reasons for punishment in the Criminal Justice Act 2003, Section 142 and constitutes a reason for appellate review of an imposed punishment. Clarkson, Keating and Cunningham (n 27) 4-5, 56-7; Herbert L. Packer, *The Limits of the Criminal Sanction* (Stanford University Press, Stanford 1968) 264.

[106] Strong (n 16) 187-8; Philips (n 17) 402; Garland (n 97) 8-9.

[107] Douglas N. Husak, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press, Oxford 2008) 89.

[108] Duff (n 22) 12, 19, 57; See also Honderich (n 9) 17-20; Daniel Farrell, 'Paying the Penalty: Justifiable Civil Disobedience and the Problem of Punishment' (1977) 6 Philosophy & Public Affairs 165, 167; Michael Davis, 'How to Make the Punishment Fit the Crime' (1983) 93 Ethics 726, 728.

[109] The concept of deserved punishment has been in its purest justified as an intrinsic good per se or an act cancelling the criminal act. Honderich (n 9) 23-5.

aim of utilitarian prevention, which is employed to specify the possible limits of penalties, when punishment is individually discussed, taking various contextual circumstances into account.[110] Desert functions as a more particularised justification, legitimising and restricting the exercise of the state's punitive power and assisting in distinguishing between the specific offender and the general offence description.[111] The main issue with just deserts has been to match the punishment to the crime[112] and solutions are given by taking two factors into account: harm and moral culpability.[113]

3.2 Harm and culpability

Harm can be defined as the violation or endangerment of a person's legal interest, which consists of all those things in which she has a stake.[114] The existence of an important harm has been deemed a basic precondition for punishment and is also crucial in proportionality assessments, since the infringement of rights that punishment entails could not be solely justified by the state's purpose of morally improving its citizens.[115] However, the various models that have been promulgated in an attempt to find ways for assessing harms proportionately have been criticised as incomplete and inefficient when applied generally to all instances of potential criminal harm, since different cases call for different standards.[116] The most commonly discussed attempt to find some standards for assessing the extent of harms is von Hirsch's 'quality of life' theory. Despite not having avoided criticisms like all the other theories,[117] this theory offers a perspective that is applicable to the activities examined here and can also assist in understanding how harms could be graded.

Evolving from his previous theory, which was based on intrusions on personal choices, von Hirsch's view focuses on interests relating to the quality of life, which are both basic

[110] Clarkson, Keating and Cunningham (n 27) 52-3; Norrie (n 34) 208, 210.
[111] Norrie (n 34) 209.
[112] ibid 212.
[113] Honderich (n 9) 35; Kleinig (n 9) 200-3.
[114] See: Joel Feinberg, 'Harm to Others' (1987) The Moral Limits of the Criminal Law, Vol. 1 *cited* in Clarkson, Keating and Cunningham (n 27) 13; Androulakis (n 7) 62.
[115] Androulakis (n 7) 61-2.
[116] Hart (n 20) 163.
[117] See Nigel Walker, 'Legislating the Transcendental: von Hirsch's Proportionality' (1992) 51 The Cambridge Law Journal 530*;* Norrie (n 34) 214.

and commonly conceived.[118] His ‘quality of life’ theory parcels together economic and non-economic interests upon which offences impinge and gauges the significance of those interests in the person’s living standard, which is constituted by four elements: ‘physical integrity, material support and amenity, freedom from humiliation and privacy’.[119] Additionally, von Hirsch provides four levels that relate to the degree of impact the harm can cause, namely ‘subsistence, minimal well-being, adequate well-being and enhanced well-being.’[120]

The combination of the elements constituting the living standard with the four levels of impact of the harm on those elements offers a guide for assessing the level of imposition on the victims’ quality of life and, consequently, the immorality of the harm. Nevertheless, as Ashworth argues, crime involves not only harm to the victim, but also to society and, therefore social consequences should also feature in assessments of harmfulness.[121] This realisation of the social implications of an action as part of the overall calculation of harm will be a very useful aspect in the discussion of hacktivism, since a protest might initially seem harmful to a party’s rights, but its potential social benefits could be considered to outweigh the victim’s harm, thus, influencing the degree of deserved punishment. Although complex to calculate, harm assessments are crucial for the criminal justice system, as they ensure that attention is given to the more important cases, saving resources from pursuing non-serious wrong-doers and trivialising the criminal process.[122] Moreover, assessments of harm relate closely to proportionality, which is important for avoiding populist punitive excesses, even if employed as a side-constraint, with the interplay of both these considerations playing a crucial role in the preservation of fairness in society.[123] Of course, as will be seen in the next chapter, the current situation has largely adopted different assessment processes that are also compromising the aims just described.

On the other hand, moral culpability is usually perceived, rather simplistically, as the responsibility for violating a valid law where there are no formal justifications or excuses that could render the act ultimately justifiable (self-defence, necessity) or exculpate the

[118] Andrew von Hirsch, '*Censure and Sanctions’* (Oxford University Press, Oxford 2003) 30.
[119] ibid 31-2.
[120] ibid 32.
[121] Andrew Ashworth, 'Some Doubts About Restorative Justice' (1993) 4 Criminal Law Forum 277, 284.
[122] Andrew Ashworth, 'Is the Criminal Law a Lost Cause?' (2000) 116 Law Quarterly Review 225, 244.
[123] ibid.

perpetrator (mental illness, duress).[124] As has been argued, 'whether a criminal defendant actually causes harm is immaterial to whether he should be deemed to have violated the criminal law and is likewise immaterial to the amount of punishment he should receive.'[125] According to this view, the ultimate extent of punishment is related to the blameworthiness of the perpetrator, the lack of which could render even harmful acts exonerated. Ultimately, culpability is defined by considerations of purposefulness, indifference to consequences or recklessness, and also by the state's duty of humanity and the judicial system's need to facilitate justice.[126] Schopp also identifies various elements that constitute the punitive process and highlights that, beyond reflection on formal, institutional proscriptions of behaviours as punishable, there are additional important contextual, practical and moral considerations to be assessed in relation to culpability at the level of specific application.[127]

The courts are supposed to take account of additional moral and factual elements, which can influence the degree of blameworthiness and consequently, modify the extent of punishment, thus, leading to mitigation or exoneration, even if formal legal defences and excuses are not totally satisfied.[128] As will be seen in the next chapter, the full applicability of formal justification defences or excuses will, in the vast majority of cases, be inapplicable or unacceptable and, therefore, the informal contextual elements that modify blameworthiness play a crucial role in deciding the ultimate extent of punishment for hacktivists.

Consequently, moral culpability is also a complex assessment process, as is assessing harm, with the two evaluations impacting on the final decision of the deserved punishment. The above discussion of harm and moral culpability allows us to realise the full scope that

[124] John Gardner, 'Crime: In Proportion and in Perspective ' in A Ashworth and M Wasik (eds), *Fundamentals of Sentencing Theory* (Clarendon Press, Oxford 1998) 43.

[125] Larry Alexander, Kimberly Kessler Ferzan, and Stephen J Morse, *Crime and Culpability: A Theory of Criminal Law* (Cambridge University Press, Cambridge 2009) 3.

[126] Andrew von Hirsch, '*Censure and Sanctions'* (n 118) 30; Gardner, 'Crime:In Proportion and in Perspective' (n 12) 43.

[127] Robert F. Schopp, *Justification Defenses and Just Convictions* (Cambridge University Press, Cambridge 1998) 23-4.

[128] Gardner, 'Crime: In Proportion and in Perspective' 37-39; For example some argue that mitigation of punishment might be seen as compensation towards a suffered distress from a social injustice having led to law-breaking. See: Edward W. Strong, 'Justification of Juridical Punishment' (1969) 79 Ethics 187, 193-4.

shapes just desert, based on an actual, generally considered condemnation process, the complexity of which also evidences the broad discretionary potential of courts in ultimately making punishment decisions by relying on much more than just the deliberate violation of a positive law. Just deserts justifications are, thus, integral in maintaining justice and providing proportionate punishments,[129] but also require an interpretive schema from which they derive legitimacy and substantiate the reason for the need to promote proportionate punishments. Two interpretations of just deserts that have moved from the narrow vengeful approach of retribution are currently prominent and can help us better understand how just deserts could function regarding the extent of punishment hacktivists would deserve. The first involves the elimination of unfair advantage and the second the communication of censure.[130]

3.3 Desert justifications and their relation to hacktivism

3.3.1 Fair distribution theories, punishment and hacktivism

Fair distribution theories are based on the presumption of a mutual agreement between citizens to maintain a fair and just balance of benefits and burdens, similar to the fairness theory of Rawls.[131] A reciprocal self-restraint is required in order for the members of society to maintain this social balance without victimising their co-citizen, while benefitting from their restraint.[132] Punishment is imposed in order to restore equality and fairness in the distribution of rights and obligations that has been compromised by the gains of the offender who has ignored his personal obligations to his co-citizens. Essentially, the state is built, and operates, on the existence of a reciprocal trust between citizens and is obliged to punish every act that undermines this trust.[133] The deservedness of punishment is calculated according to the extent of the imbalance of benefits and obligations that is generated between the perpetrator and the rest of society.

[129] Clarkson, Keating and Cunningham (n 27) 29-30; Walker (n 117) 531.

[130] Clarkson, Keating and Cunningham (n 27) 26-8.

[131] See Ch 2, Part ***2.2.2 Social contract theories: From Hobbes to Habermas and Rawls***.

[132] von Hirsch, *Censure and Sanctions* (n 118) 7; Honderich (n 9) 54-5.

[133] Duff (n 22) 23.

Applied to cases of morally motivated political acts like ECD, the imbalance of rights caused from law-breaking could be mitigated by the demonstration of moral, altruistic motivations of the protesters that do not benefit personally or make profit from their law-breaking, while also risking imprisonment. ECD focuses, in principle at least, on promoting common well-being and justice. Therefore, the immorality of violating rights through the protests is morally outweighed by the socially beneficial, rights-promoting goals of the protesters, who often aim to restore an already disturbed balance of rights and obligations, caused by the injustice protested. In addition to that, of course, hacktivism entails expressive elements, being partly considered an exercise of rights in itself. Moreover, the fact that protesters potentially avoid being considered seriously reprehensible for meddling with the social balance of rights is reinforced by the already existing social imbalances, which are admittedly inherent in man-made social systems.[134] As Norrie argues, 'one cannot judge legal equality properly in abstraction from the overall social context in which it operates.'[135] Consequently, based on already existing imbalances of rights, even legally ambiguous attempts at restoring an already disturbed balance would be expected and potentially be considered justifiable.[136] Contextual assessments of harm and moral culpability should not be based on an abstract, ideal equality of burdens and benefits. Instead, the current, imbalanced social conditions should be considered a starting point for proving whether the equilibrium of rights and obligations is further disturbed or partly restored by the protesters.[137]

Furthermore, activists and hacktivists often put their liberty and enjoyment of rights and benefits at potential risk by openly engaging in legally ambiguous activities that can lead to their monitoring, prosecution and even imprisonment.[138] Therefore, their disturbance of the balance of rights through their disobedience is outweighed by the risk they take that society might restrict their rights and liberties analogously through punishing them for their protests. As Mill has suggested, instead of feeling disadvantaged by these types of offenders, one should feel grateful or, at least, sympathetic towards them for

[134] Rawls (n 2) 173; Honderich (n 9) 56.
[135] ibid 212.
[136] Some even argue that mitigation of punishment might be seen as compensation towards a suffered distress from a social injustice having led to law-breaking. Strong (n 16) 193-4.
[137] Norrie (n 34) 211.
[138] Ravi Somaiya, 'Activists Say Web Assault for Assange Is Expanding' (*The New York Times,* 10 December 2010) <http://www.nytimes.com/2010/12/11/world/europe/11anonymous.html?_r=4> accessed 16 Januray 2010; Goldstein (n 39).

shouldering the risk of punishment in order to challenge prevailing interests and protect the common welfare.[139] Moreover, even if hacktivists are considered to be compromising online trust by disturbing the accessibility/functionality of commercial and governmental websites, thus, impacting adversely on the rights of Internet users, their practices can simultaneously be considered to ultimately promote systems integrity and trust in cyberspace, eventually supporting user rights such as security, privacy of communication and free expression. For example, hacktivists have often attempted to unveil potential weaknesses in the security systems and operation of websites, incentivising website moderators and companies to improve security and educate citizens in the potential privacy risks in communicative networks.[140]

Hacktivist groups also resort to acts that eliminate other dangerous illegal activities online, such as online child pornography.[141] These efforts would, thus, promote trust by ultimately reducing the risks for infringement of users' rights en masse, as hacktivists would induce the increase of security of websites and computer software. For example, Hacktivismo and its mother hacker group Cult of the Dead Cow have often generated software, such as Back Orifice or Goolag Scanner in order to highlight or identify software and website weaknesses and force companies or help owners to patch these holes before being compromised by some more malign user.[142] Furthermore, hacktivist protests could even promote social trust, by attempting to bring citizens together to deliberate and protest for common causes, thus, intensifying a sense of solidarity in the online community, as well as mutual respect and understanding through the diversification of discursive processes.[143] In demanding freedom of information, transparency and public accountability

[139] Brownlee 'Civil Disobedience' (n 37); Colby (n 68) 1168.

[140] See Trevor Thompson, 'Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the White Hats under the CFAA' (2008) 36 Florida State University Law Review 537, on how ethical hacking could lead to more security, if promoted. See also Mathias Klang, 'A Critical Look at the Regulation of Computer Viruses' (2003) 11 International Journal of Law and Information Technology 162 regarding the potential benign uses of viral software.

[141] Violet Blue 'Anonymous Attacks Child Porn Websites and Publish User Names' (*ZDnet Blog,* 21 October 2011) <http://www.zdnet.com/blog/violetblue/anonymous-attacks-child-porn-websites-and-publish-user-names/757> accessed 19 February 2012.

[142] Hacktivismo, 'Hacktivismo Projects' (*Hacktivismo,* undated) <http://www.hacktivismo.com/projects/index.php> accessed 01 December 2012.

[143] David Mead, *The New Law of Peaceful Protest: Rights and Regulation in the Human Rights Act Era* (Hart Publishing, Oxford 2010) 7. For example, the central message of Anonymous is that everybody can participate in any of the actions through globally-coordinated actions both on and offline towards common interest goals.

of power-yielding factions, hacktivism facilitates openness and improved communication between the state and citizens, and unveils and potentially induces amelioration of pertaining imbalances of rights and obligations between social groups. Therefore, their beneficial effects and moral motivations would essentially positively influence just deserts assessments, suggesting the need for more lenient punishment.

Although in principle hacktivism could entail the socially beneficial, moral characteristics described above that would positively influence just deserts assessments, the radicalisation of hacktivists and the abandoning of morally justifiable practices could reverse the impression that hacktivists care for the public welfare and the promotion of trust and equality in cyberspace. As will be seen in the next chapter, the simultaneous demonisation of protesters by the authorities and the media, reinforced by morally problematic tactical choices and rhetoric on the hacktivists' behalf, can alienate the public and generate a feeling of unfairness and fear in other citizens regarding the nature and consequences of hacktivist actions. If hacktivism is perceived as intensifying, rather than mitigating, the imbalance of rights in society, higher punishment assessments would reflect that intensification of mistrust. For example, if hacktions cause increasingly damaging effects that create an even more intense disturbance of rights in their victims and society without any defined political benefit, then their claim to deserving mitigated punishment would be substantially weakened. As a general rule, though, if the deservedness of punishment for ECD is based on the balance of rights, it can appear that for hacktivist actions that abide by the moral standards discussed in the previous chapter, the nature of the punishment ought to reflect a less morally culpable behaviour and reduced harmfulness.

3.3.2 Communication theory, punishment and ECD

Communication theory of punishment is a hybrid that can combine utilitarian with retributive elements, but can also be predominantly backward-looking.[144] Since utility has already been discussed,[145] I will focus on its retributive aspect. Communication theories

See: Anonymous, 'Anonymous Declaration of Freedom' (*Whyweprotest,* 10 January 2011) <http://www.whywefight.net/2011/01/10/anonymous-declaration-of-freedom/#axzz2HrN1bzrV> accessed 10 January 2011.

[144] Garland (n 97) 9; Walker (n 117) 532.

[145] Part
2.2 Preventive functions and ECD.

justify punishment as a form of public censure that the state imposes to express the moral condemnation of society towards offenders, who, as rational moral agents, realise their fault and accept punishment as deserved and, thus, justly imposed.[146] This theory encompasses the fair distribution elements of depriving the offender of his advantage through punishment and further enriches it by introducing a blaming function.[147] The functions of blaming and internalisation of the moral harm perpetrated seem to also encompass the emotive satisfaction of victims and expiation of offenders through their acceptance of blame, which have been considered in the past as backward-looking justifying aims of punishment.[148] Furthermore, the focus on blame is important in discussing hacktivism, since the potentially reduced moral blameworthiness of the perpetrators immediately translates to reduced public censure and thus more lenient responses.[149]

As von Hirsch submits, censure-based theories generally promote lower punishments per se, since extreme penalties would alienate the offender and, consequently, reduce the communicability of moral disapproval.[150] The communication theory also views punishment as a continuous process that does not just relate to the final sanction, but is constituted from the whole ordeal of going through the criminal justice processes that entails censure.[151] Punishment is, thus, partly constituted by the publicisation of the processes of arrest, prosecution and trial, which, being harmful for the suspect, communicate a certain degree of moral disapprobation, even before the actual punishment and even if, ultimately, punishment is not imposed.[152] Therefore, one would suggest that the final sentence would be more lenient, as it would be considered only a part of the overall censuring process, with the final sanctions imposed by courts being mitigated after taking into account the additional harm suffered by the defendant that undergoes all the criminal justice processes.

[146] Kimberley Brownlee, 'The Communicative Aspects of Civil Disobedience and Lawful Punishment' (2006) 1 Criminal Law and Philosophy Journal 179, 185; Duff (n 22) 28-9.

[147] Clarkson, Keating and Cunningham (n 27) 28.

[148] Apart from the already mentioned dominant retributive interpretations, retribution has often been articulated as expressive of the vengeful sentiment of people towards unsocial members of society or in the form of expiation that punishment realises, as a redeeming act for the immorality of the perpetrator. ibid 24-5.

[149] von Hirsch, *Censure and Sanctions* (n 118) 9.

[150] Andrew von Hirsch, 'Proportionate Sentences: A Desert Perspective' in Andrew Ashworth and Andrew von Hirsch (eds), *Principled Sentencing: Theory and Policy* (Hart Publishing, Oxford 1998) 171.

[151] See (n 66)

[152] Husak (n 107) 5-6, 13; von Hirsch, *Censure and Sanctions* (n 118) 25-6.

There are, thus, prima facie reasons related to the justification rationale per se suggesting mitigated punishments, compared to purely retributive, vengeful versions that existed previously. However, there are obviously hacktivism-specific reasons that influence the extent of punishment regarding this punishment rationale.

Moral condemnation and, respectively, the extent and harshness of punishment could be moderated by the lack of a general acceptance of censuring hacktions. For example, US state officials have acknowledged that hacktions have more similarities than differences with regular, offline protests, which are also often disruptive and cause social inconvenience.[153] Beyond political activists, who would usually be positively inclined towards moral hacktivism and the fact that especially virtual sit-ins are joined by thousands of participants,[154] even academics, elected politicians and even some state officials have viewed hacktivism as no more than a nuisance or a new political tactic that could be considered non-dangerous in many cases.[155] As Morozov further argues, in order to assess the deservedness of lenient punishment of virtual sit-ins, the focus should not be on the medium (the law-breaking act), but on the message (the moral cause promoted).[156] Moreover, even German courts have in the past declared virtual sit-ins as legitimate expression and have exonerated the protesters from any liability.[157] Admittedly, the cybercrime regimes in Germany and globally have become much stricter towards virtual sit-ins currently,[158] nevertheless, the case is indicative of the existing view that virtual sit-ins

[153] Dominguez, 'Electronic Disobedience Post-9/11' (n 60); Josephine Wolff, 'Interview: Howard Schmidt' (*MSNBC,* 21 December 2010) <http://www.newsweek.com/2010/12/21/interview-with-cyber-security-czar-howard-schmidt.html> accessed 18 January 2011; Alex Newman, 'Hacker Group Takes on Fed, IMF, "Global Banking Cartel"' (*The New American,* 15 March 2011) <http://www.thenewamerican.com/tech/computers/item/7213-hacker-group-takes-on-fed-imf-global-banking-cartel> accessed 12 August 2011.

[154] See the numbers of participants for the various protests organised in Ricardo Dominguez, 'Electronic Civil Disobedience' (*thing.net,* undated) <http://www.thing.net/~rdom/ecd/ecd.html> accessed 16 January 2011.

[155] Wolff, 'Interview: Howard Schmidt' (n 153); Crosstalk (n 4);Evgeny Morozov, 'In Defense of DDoS' (*Slate Magazine,* 13 December 2010) <http://www.slate.com/id/2277786/> accessed 20 May 2011; Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Jon Arquila and David Ronfeldt (eds), *Networks and Netwars:The Future of Terror, Crime, and Militancy* (RAND Corporation, 2001) 269; Alexandra W. Samuel, 'Hacktivism and the Future of Political Participation' (DPhil Thesis, Harvard University 2004) 244-5.

[156] Morozov, 'In Defense of DDoS' (n 155).

[157] European Digital Rights, 'Frankfurt Appellate Court Says Online Demonstration Is Not Coercion' (*European Digital Rights*, 07 June 2006) <http://www.edri.org/edrigram/number4.11/demonstration> accessed 20 May 2011.

[158] Ch 4, Parts 3.1 The making of cybercrime laws and.3.3.1 The focus on damage and loss and the expansion of the scope.

realised under moral criteria can even be accepted as protectable free expression.[159] The potential acceptability and understanding of the motives of hacktivists by a large percentage of the public, even if still a minority,[160] would, under the communication theory, render public censure weaker and would, thus, not justify high imprisonment penalties, leading instead to mitigated sentences or non-prosecutions.

Public disapprobation could be intensified if the reports surrounding such activities are dramatic and exaggerated by the media and security firms intensifying technology-related moral panics,[161] while the usefulness of the protests might not be directly obvious.[162] The lack of knowledge or the capacity to understand the intricacies of online political activities, such as hacktivist actions, could also reinforce the popular tendency to condemn ECD, since the general public will be able to perceive these actions as purely cybercriminal offences. After all, despite the fact that a substantial minority is positive towards hacking, the majority still appears negatively inclined towards hacking-related actions[163] and as seen above,[164] the lack of detailed knowledge of the cases in question could lead the public to adopt harsher solutions.

However, although the public can be portrayed as generally punitive, research has shown that, when the public is informed about specific incidents and potential alternative penalties, they tend to prefer more lenient penalties.[165] Although the wider public might not be familiar with the specifics of hacktivist actions, the fact that there are various voices from various influential sectors of society that express their reluctance to overtly condemn these activities means that one could argue that the public might be torn as to the immorality and dangerousness of these acts and, therefore, the social censure towards hacktivists could be reduced overall, thus, justifying less serious punishments.

Furthermore, since the protesters' targets are considered to be shaping socio-political and economic realities, society could more easily accept the expression of dissent towards

[159] Ch 2, Part 1. Free expression and hacktivism.

[160] A substantial minority of the polled public has indicated an accepting attitude towards hacking, even without some moral political goal behind these acts. Dowland et al. (n 74); Yar, 'Public Perceptions and Public Opinion About Internet Crime' (n 73) 113-4.

[161] Yar, 'Public Perceptions and Public Opinion About Internet Crime' (n 73) 107-112.

[162] For more on exaggerated reports see Ch 4, Part 2.3 The influence of the media, experts and security firms.

[163] Dowland et al. (n 74) 720.

[164] See (n 79).

[165] ibid.

the politically influential factions that are considered to promote unjust or socially harmful policies.[166] Moreover, in many cases, purely legal protests, such as strikes and marches in real-life, could prove far more disruptive for citizens than illegal ECD and generate much more public disaffection than an illegal online disruption. Citizens are likely to be much less morally accepting towards a strike in the public transport sector than towards a virtual sit-in on the website of the Ministry of Transport, due to the much lesser disruption and inconvenience the online protest would cause, compared to the offline strike, even if the online protest is illegal, while the offline is legitimate.[167] Additionally, tolerance of disobedience could also result from historical precedent. Particularly in western liberal societies, like the US, which have accepted and often embraced a deep tradition of CD, moral disapproval could also be lesser due to the familiarisation of society with political disobedience and the acknowledgment that similar practices have led to important social changes.[168]

However, increased blaming could also ensue if citizens become aggrieved by persistent or seriously disruptive attacks on governmental websites, especially in times when nationalist sentiment runs high and terrorist threats dominate public fears. Regarding commercial websites, downtime could cause significant losses, which could be easily translated into public censure, on the premise that commercial damages would eventually have an impact on consumers in addition to delays in access.[169] Loss of business and reparation costs could arguably sometimes be so high as to have cascading effects, such as

[166] Brownlee, 'The Communicative Aspects of Civil Disobedience and Lawful Punishment' (n 146) 180; Colby (n 68) 1175; For example, the disregard for environmental safeguards and labour laws by big corporations could generate intense moral disapproval towards these companies, which could mitigate the social reprobation that legally ambiguous protests against unjust corporate policies could generate.

[167] The public would be much less accepting towards a strike in means of public transport than towards a virtual sit-in on the website of the Ministry of Transport, due to the much lesser disruption and inconvenience the online protest would cause, even if the protest online is illegal and the offline legal.

[168] Hannah Arendt, *Crises of the Republic* (4th edn, Harvest Books, San Diego 1972) 80-1; Mead (143) 12.

[169] That is one of the reasons Anonymous argue they never protested against Amazon, during their Wikileaks protests, as such a protest, even if feasible in terms of resources, - something doubtful due to the resilience of the Amazon network - would frustrate people using the website for their shopping. Charles Arthur 'Inside 'Anonymous': Tales from within the Group Taking Aim at Amazon and Mastercard' (*Guardian Technology Blog,* 13 December 2010) <http://www.guardian.co.uk/technology/blog/2010/dec/13/hacking-wikileaks> accessed 19 December 2012.

price increases and job losses;[170] phenomena that would fuel moral censure towards hacktivists. In order to cause these cascading effects, though, disruptive acts will usually have to be severe and persistent in order to consistently hinder the function of the websites targeted.[171] As Kessler, equity analyst at Standard & Poor's has argued, most of the companies that will be targeted by protesters will be well prepared to withstand such attacks so their operations will not be adversely affected.[172]

Moreover, there is a possibility that high losses will be incurred, not as a normal aim of the protest, as with regular, intentional criminal acts, but as an unavoidable collateral damage for realising ECD,[173]or the result of reckless/negligent behaviour or unpredictable events. After all, with protests that manipulate code or that are open to the public, it is very difficult to gauge the actual impact a defacement or a sit-in could have on different websites or the time and cost that restoring a system could take for different cybersecurity services. The potential unpredictability of damage, therefore, could also generate public concern and censure, even if that censure would often incorporate the mitigated moral reprehensibility that recklessness, negligence or unpredictability entail. When any damaging or vengeful intention is missing, censure would less often develop into a full condemnation to be reflected on the extent and nature of sanctions that are imposed.[174] After all, criminal law has always suggested more lenient responses towards recklessness or negligence or unforeseen results, acknowledging both a reduced need to prevent such phenomena and also a reduced moral blameworthiness.[175]

[170] Brian Cashell et al., *CRS Report for Congress: The Economic Impact of Cyber-Attacks* (Government and Finance Division, 2004) <http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf> accessed 24 February 2013.

[171] Amazon was virtually unhindered by the protests of Anonymous and was not attacked again after that.

[172] Jeff Bliss and Justin Blum, 'Holder Says U.S. Probes Wikileaks-Related Web Attacks' (*Bloomberg,* 9 December 2010) <http://www.bloomberg.com/news/2010-12-09/holder-says-u-s-is-looking-into-wikileaks-tied-cyber-attacks.html> accessed 16 January 2011.

[173] See Ch 2, Part 1. Free expression and hacktivism, for the lack of public spaces online, making hacktivist protests more natural also Part 3.2 Non-violence for the argument that all CD entails some measure of coercion that could generate damage.

[174] Skibell (n 48) 943; Columbia Law Review Association (n 37) 1510; If, for example, one believes his actions are justified based on unreasonable grounds, which would not suffice for a full justification defence the crime is mitigated to the respective offence prosecuted for negligence. Model Penal Code, Section 3.09.

[175] Compare penalties of murder and manslaughter, where motivation differs. See 18 U.S.C. 1111-2, ranging from life for murder to 10 years for manslaughter.

In conclusion, it appears that morally acting ECD protesters could often be considered deserving of lenient punishments, because their generally genuine political motivations and the usually socially considerate nature of their activities would generate less social reprobation to be communicated through punishment. However, the predicted reduced censure is not unconditional. The tactics employed could generate censuring reactions, even beyond the act of violating a valid law, which prima facie gives rise to some degree of moral censure in any case. If the protests are realised regardless of the moral criteria that influence justifiabilty – an assessment which will demand individual, contextual evaluations - high censure could easily ensue.[176] One could, therefore, submit with more certainty now that lengthy custodial penalties and generally harsh punishments would not only often be potentially inefficient or even counterproductive when imposed on legitimate hacktivist efforts, but would also be disproportionate and unjust, according to concerns regarding he deservedness and moral culpability of the offenders.

4. Conclusion

This chapter discussed the major justifying reasons for punishment. It established important reasons both on the basis of utilitarian prevention and just deserts which indicate that lenient punishments that would not entail lengthy incarceration would generally be more justifiable for moral hacktivists. It is gradually becoming apparent that, if the adopted solutions are to protect the public well-being as well as the rights of protesters and the rule of law and the legitimacy of democracy in general, there are many complex considerations to be taken seriously in formulating criminal policies and regulation. These considerations are influenced by the whole normative and enforcement structure of the legal system and its capacity to facilitate a reasoned balancing of deontological and consequentialist considerations.

The assessment of whether the current regulatory regime offers the chance for accommodating contextual assessment, distinctions in terms of harmfulness, motivation and ethical background and even tolerance and leniency to political activism and network modifications is linked to many different elements, from the nature and scope of the

[176] Brownlee, 'The Communicative Aspects of Civil Disobedience and Lawful Punishment' (n 146) 190.

specific legal framework to additional external socio-political conditions and practical realities that shape the perceptions and actions of citizens, private actors, criminal justice officials and even hacktivists themselves. The following chapter will give us a clearer image of how the current system operates and influences hacktivism and whether the current regulatory tools employed are appropriately efficient and just in order to accommodate the elements of contextual assessment, leniency and tolerance, but also overall security, user rights and crime prevention.

CHAPTER 4
THE CURRENT REGULATORY APPROACH TO HACKTIVISM: ANALYSIS AND CRITIQUE

The previous chapters reviewed the nature of hacktivism, its role as a modern manifestation of counter-power in cyberspace and established that hacktivism is an alternative online political practice that, when following certain moral standards, could be justifiable and politically useful. Subsequently, the thesis attempted to assess whether harsh and exemplary punishments, focused on incarceration, would be justifiable when applied to hacktivist practices, both from a utilitarian prevention and a just deserts perspective. Eventually, this analysis demonstrated that more lenient penalties and tolerant approaches would often be more appropriate and justifiable, in terms of crime prevention and overall utility as well as in terms of the moral censure hacktions generate, than harsh penalties, predominantly expressed in the form of long-term imprisonment. Another important finding, thus far, is that the fluidity and diversity of hacktivism in terms of perpetrators, motivations and tactics, essentially renders assessments of the justifiability of hacktivist actions related to the specific context of the protest, both in terms of protester blameworthiness but also in terms of conditions that render the act worthy of prevention and essentially disutilitarian. Subsequently, this means that the promotion of opportunities for discretion in addition to a capacity for demonstrating leniency and tolerance would be considered crucial for achieving more just and efficient results when dealing with hacktivism.

The purpose of this chapter will, thus, be to assess whether the approach currently followed in relation to hacktivism facilitates the existence of objective assessments of cyberdeviants, an understanding of the inevitable role of hacktivism for modern, online societies and the capacity to exercise discretion and demonstrate leniency and tolerance for these political activities. In order to achieve such an assessment, the chapter will discuss direct and indirect regulating influences, such as the impact of dominant socio-political symbolisms and norms, before moving to analyse the structure and focal points of cybercrime laws and their potential for allowing lenient approaches. Furthermore, this chapter will review whether the norms, political dictates and practices that prosecutors and judges are influenced by, allow for unbiased contextual assessments, the acceptance of controversial moral and political views and the preference for more lenient and alternative forms of punishment. The role of private companies in reinforcing such norms and processes will also be discussed. Before we proceed with the assessment of the specific aspects of the current regime, however, the regulatory approach adopted, which is predominantly focused on traditional notions of 'command and control' regulation through the employment of the criminal justice system, needs to be clarified.

1. Regulating hacktivism: The focus on 'command and control'

The review in Chapter One of general regulatory suggestions in relation to networks such as cyberspace has highlighted the particular need to promote a decentralised and multi-actor approach to regulating online phenomena.[1] The general shift towards more decentralised models of regulation also relates to the networked, decentralised nature of cyberspace that with its global nature inevitably challenges even more the already challenged state-based forms of regulation.[2] However, irrespective of expectations of decentralisation, which have, perhaps, materialised much more in areas, such as preventing copyright infringement,[3] there seems to be a persistent trend to deal with hacktivist incidents through a more traditional, criminal law-based 'command and control' approach. This approach relates to

[1] See Ch 1 Parts 1.1 Defining regulation and 1.2 The modern networks.

[2] For decentralised regulation see for example: Clifford Shearing and Jennifer Wood, 'Nodal Governance, Democracy, and the New 'Denizens'' (2003) 30 Journal of Law and Society 400; Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a" Post-Regulatory" World' (2001) 54 Current Legal Problems 103; John Braithwaite, *Restorative Justice and Responsive Regulation* (Oxford University Press, Oxford 2002); For cyberspace, multi-actor regulation see: Lawrence Lessig, *Code v.2.0* (Basic Books, New York 2006); Henry H. Perritt Jr, 'Towards a Hybrid Regulatory Scheme for the Internet' (2001) 2001 The University of Chicago Legal Forum 215; Joel R. Reidenberg, 'Technology and Internet Jurisdiction' (2004) 153 University of Pennsylvania Law Review 1951.

[3] Piracy prevention measures are a mix of legislation of extending copyright and increasing sanctions, lawsuits, technological filters of websites such as ThePirateBay and Internet Service Provider monitoring of use and imposition of informal sanctions.

the use of state legal rules backed by criminal sanctions,[4] with the state promulgating orders and imposing penalties, and the other actors involved, directly or indirectly, from actual hacktivists to private online intermediaries obliged to abide by the these state orders.[5] For example, as will be seen throughout this chapter, even when private actors are asked to participate in the regulatory process, this is predominantly realised as a reaction to a legal or executive command, in order to avoid legal and political consequences flowing from non-compliance with the authorities' desires.[6]

Yet the choice of a 'command and control' approach is seemingly made regardless of the inherent deficiencies of such regulatory approaches in general and in cyberspace more specifically. Black has identified some of the most common problems for state-based regulation. She argues that law can be poorly targeted or too unsophisticated to deal with complex problems (instrument failure), there can be insufficient knowledge on behalf of state actors involved in identifying the causes of problems and generating solutions or identifying non-compliance (information and knowledge failure), and also inadequate implementation of the designated measures (implementation failure).[7] As will become obvious from the following analysis, these deficiencies are evident in the cybercrime law regime and in dealing with hacktivism in particular, since the moral characteristics of hacktivism and the practical difficulties posed by cyberspace more generally probably generate even more challenges for state-based legal regimes than in most other areas. As was discussed during a recent cybersecurity conference, law enforcement and general regulatory efforts are still challenged by simple cases of plain criminality online, such as criminal hacking, identity theft, extortions and computer damage attacks, which are also much more numerous and serious than political hacks.[8]

[4] Julia Black, 'Proceduralisation and Polycentric Regulation' (2005) Especial 1 RevistaDIREITOGV <http://direitogv.fgv.br/sites/direitogv.fgv.br/files/rdgv_esp01_p099_130.pdf> accessed 16 December 2012 102.

[5] ibid.

[6] See Part 4. The role of private actors.

[7] Black 'Proceduralisation and Polycentric Regulation' (n 4) 102; Julia Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 2.

[8] See Conference Reports in Warwick Ashford, 'Infosec 2013: Cyber Crime Challenges Law Enforcement' (*Computer Weekly,* 25 April 2013) <http://www.computerweekly.com/news/2240182575/Infosec-2013-Cyber-crime-challenges-law-enforcement> accessed 20 June 2013.

Challenges to cybercrime laws have been a core issue since the early regulation debates between Johnson and Post,[9] on the one hand and Goldsmith,[10] on the other. Some of the main considerations were inevitably related to the decentralised and global nature of the medium that posed serious practical difficulties to any attempts to regulate through national laws. The problems range from difficulties in identifying perpetrators to jurisdictional conflicts that lead to 'forum shopping' tactics, thus, eventually minimising the efficiency of national legislation in regulating cyberspace.[11] Another important problem that flows from the jurisdictional conflicts is the presumed democratic deficit of enforcing national criminal laws globally, leading to further illegitimacy concerns. As Post and Johnson argue, regulation through state laws could have spill-over effects on citizens, who have not consented to the sovereign imposing those laws on them and have received no notification on the applicability of these laws.[12] Reed also argues that the general acceptance of general user norms or the creation of laws entailing qualities that will command the public's respect are crucial for regulatory success, since, on the Internet, the lack of acceptance by a substantial number of online actors could compromise the overall legitimacy and acceptability of a whole legal regime and not just a regulatory choice.[13] Maintaining legitimacy and public acceptability of mandatory cybercrime provisions is a challenge that is still pertinent considering global cybercriminality and, as will be seen throughout the chapter, the crackdowns against hacktivists are reducing the weak claims of legitimacy that the already broadly reaching cybercrime regimes have.

Even Goldsmith, who supports the idea that existing laws and traditionally employed ways for the state to enforce its laws beyond its borders, thus allowing for national laws to be employed to regulate cyberspace activities,[14] also accepts that cyberspace can pose serious challenges to legal systems.[15] Yet he argues that, despite any flaws, especially for issues of mandatory, criminal law, state laws could help regulate according to established rule of law principles in order to protect the rights of others from excesses inherent in

[9] David Johnson and David Post, 'Law and Borders--the Rise of Law in Cyberspace' (1995) 48 Stanford Law Review 1367; David Post, 'Anarchy, State and the Internet' (1995) 3 Journal of Online Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943456> accessed 18 December 2012.

[10] Jack L. Goldsmith, 'Against Cyberanarchy' (1998) 65 The University of Chicago Law Review 1199.

[11] Johnson and Post (n 9) 1369-70 onwards.

[12] Johnson and Post (n 9).

[13] Chris Reed, *Making Laws for Cyberspace* (Oxford University Press, Oxford 2012) 17-26.

[14] Goldsmith, Against Cyberanarchy (n 10).

[15] ibid 1201.

private ordering.[16] He also accepts that enforcement can be facilitated by other mechanisms and actors, where state mechanisms are challenged.[17] Especially regarding the global divergence of laws that might cause confusion, Goldsmith highlights the need for international harmonisation as a prerequisite for the proper employment of national laws in cyberspace so as to minimise conflicts of law.[18] As will be seen below,[19] however, contemporary cybercrime regimes have greatly extended their reach beyond national borders. This extension, in addition to the increasing strictness and arbitrariness of the regimes in the US and UK, for example, essentially compromise the principles and safeguards that Goldsmith was expecting national laws would ensure, since cybercrime laws often impinge upon civil liberties and rule of law procedures and rights, while the authorities also collaborate, coerce or induce private actors to assist in these processes rather than preserve the balance by decentralising power and control.

Despite his belief in multi-actor regulation, Lessig had expressed similar fears, that during the interaction of regulatory tools and actors, the state as the traditional incumbent power, could potentially dominate the regulatory processes and propagate its desirable norms, laws and enforcement of these with the help of similarly interested or coerced private actors, from media conglomerates, to security firms and Internet service providers.[20] Reidenberg has also highlighted the potential of the state to engage with private actors in mainly employing technological controls to facilitate monitoring, enforcement and sanctioning.[21]

The rest of this chapter will analyse how the current regulatory situation, especially in dealing with the issue of hacktivism, resembles a mixture of Lessig’s fears for the role of the state in regulating online phenomena and the illegitimacy concerns of cyberlibertarians, such as Post and Johnson due to its central focus on hierarchical control and power concentration. As Palfrey argues, after the initial de-regulation period at the beginning of the Internet’s popularisation, states have gradually taken more regulatory initiatives and are not only regulating state-to-individual interactions, but are also trying to control private

[16] ibid.
[17] ibid.
[18] ibid.
[19] See Part 3. The impact of cybercrime laws on hacktivism.
[20] Lessig, *Code v.2.0* (n 2).
[21] Joel R. Reidenberg, 'States and Internet Enforcement' (2004) 1 University of Ottawa Law & Technology Journal 216.

entities and induce or coerce them to do the government's biding.[22] The subordination of almost all the nodes and tools in the regulatory network to serving particular regulatory goals based on security and information-control and established mainly by the government essentially cancel the benefits of multi-actor, decentralised regulation to a large extent and further propagates problems of efficiency and justness and ultimately, legitimacy, consequently rendering the cybercriminal justice regime an inappropriate tool for dealing with hacktivism. Let us then proceed to discuss these issues in more detail, beginning from the normative framework behind the current regime.

2. The normative framework and its impact on hacktivism

2.1 Fear of risk and security discourses

The regulation of behaviours and the shaping of laws is influenced by the pervasive socio-political norms and symbolisms and, thus, the treatment of hacktivism will initially be related to the directions posed by dominant norms and regulatory policies. Hacktivism has developed at a time, when welfarism[23] has been abandoned and governance philosophies focus instead on managing risks and increasing order.[24] Fear of crime has become a main driving force for establishing policies that attempt to reduce risk-related activities, from health and safety regulations to actual criminal offences and legitimising the gradual shift of democratic regimes towards public safety and national security.[25] As Sunstein argues,

[22] John Palfrey, 'Four Phases of Internet Regulation' (The Berkman Center for Internet & Society Research Publication Series, Research Publication No. 2010-9) http://cyber.law.harvard.edu/publications> accessed 18 December 2012.

[23] Welfarism is a mode of social organising that presupposes a dominant role for the government in providing social security for its citizens through an extensive system of taxation, social insurance and policies of wealth redistribution that are designed to safeguard against the difficulties citizens might have to face, from illness to unemployment and old age. Especially after the Second World War, social security and welfare became a general right and access to such services became universalised. Lucia Zedner, *Security* (Routledge, New York 2009) 34-5.

[24] Zygmunt Bauman, *Modernity and Ambivalence* (Polity Press, Cambridge 1991) 4; David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford University Press, Oxford 2001).

[25] Garland (n 24); Michael McGuire, *Hypercrime:The New Geometry of Harm* (Routledge Cavendish, Oxford 2007) 32; Jonathan Simon, *Governing through Crime* (Oxford University Press, Oxford 2007)

regulation is currently dominated by the 'precautionary principle', which dictates that regulators should try to protect society from hypothetical harms, even if the causal links between these harms and public safety are unclear and their realisation only probable.[26] Policies of zero-tolerance toward risk have also overwhelmed and substituted fiscal efficiency tactics that entailed increased rationalisation processes,[27] with this lack of rationality facilitating more emotive and consequently more punitive approaches.

Zedner summarises the elements of the general theory of security in criminal justice: First, there is a temporal shift towards pre-emption and reduction of criminal opportunity;[28] secondly, risk is the framework for security, with security policies mainly designed to locate and manage diverse risks;[29] thirdly, the focus of crime does not centre on wrongdoing, but aims to pre-empt and minimise loss.[30] Security becomes a commodity in the balancing between the cost of measures that promote it and the potential losses from risk-related activities and, consequently, the provision of security becomes a profit-making process.[31] This prominence of security as a measure for political and financial success is, as will be seen in this chapter, reflected on all levels, from politicians' declarations and legislative initiatives to business sector policies and the judiciary's punitive trends.

The policy-making focus on security is further reinforced by the terrorist events and relative rhetoric that have naturally proliferated, especially after 9/11, and which have fuelled public fears, due to the intensely destructive unpredictable fear-inducing effectss terrorism can have on the public.[32] Consequently, terrorist trauma facilitates the rushed, non-deliberated imposition of emergency policies.[33] Terrorist fears also strengthen the role

4; Barbara Hudson, *Justice in the Risk Society: Challenging and Re-Affirming Justice in Late Modernity* (Sage Publications Ltd, London 2003) 43-5, 49-50.

[26] Cass R. Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge University Press, Cambridge 2005) 4,15,18,21.

[27] Garland (n 24) 18-9; Manuel Castells, *Communication Power* (Oxford University Press, Oxford 2009) 28-9.

[28] Lucia Zedner, 'Pre-Crime and Post-Criminology?' (2007) 11 Theoretical Criminology 261, 265.

[29] ibid.

[30] ibid.

[31] Security contractors that have an interest in the intensification of security concerns and, thus, the need for security measures they offer and politically for governments that gain in the eyes of the public by appearing strict and supportive of order and elimination of risk. ibid.

[32] Simon (n 25) 267; Marcus J. Ranum, *The Myth of Homeland Security* (Wiley Publishing Inc., Indiana 2004) 20.

[33] Naomi Klein, *The Shock Doctrine* (Penguin Books, London 2007); See also Part 3.1 The making of cybercrime laws.

of the state as a dominant actor that is capable and burdened with managing risk control.[34] Moreover, since information is fast becoming a core resource of society,[35] the protection of information is often analogised to protecting public safety or national security.[36] Consequently, the state becomes more punitive in order to demonstrate its capacity to deal with controversial political groups[37] that are labelled as security threats.[38] Simon emphasises the danger for dissidents, arguing that the 9/11 events have often been perceived by the authorities as a license to persecute future non-violent demonstrations and to prosecute ideologically radical groups, irrespective of terrorist motivations or actions.[39] This trend is very strong in the case of hacktivism, where the state takes a more active, policing role.

The Internet, as part of our social space where citizens also interact, is unavoidably influenced by the above normative tendencies and also fuels them.[40] It feeds fears of crime and concerns for risk due to its unpredictable technological nature, which entails an inherent risk for technology to malfunction or be misused[41] and can often challenge the average citizen's capacity to understand the various phenomena of cyberdeviancy within it. This tendency is also further reinforced by the medium's inherent potential for anonymity that generates uncertainty and can hinder crime prevention.[42] The difficulty to understand, measure and predict the potential risk also magnifies the salience of cybercrime, eventually inducing the public to support more preventive and punitive measures that presumably

[34] Zedner, *Security* (n 23) 117.

[35] See Ch 1, Part 1.3 Information and power in the networks.

[36] Johan Eriksson and Giampiero Giacomello, 'The Information Revolution, Security, and International Relations:(Ir) Relevant Theory?' (2006) 27 International Political Science Review 221*,*222-4.

[37] Garland (n 24) 134.

[38] Alex Callinicos, 'The Anti-Capitalist Movement after Genoa and New York' in Stanley Arownowitz and Heather Gautney (eds), *Implicating Empire:Globalization and Resistance in the 21st Century World Order* (Basic Books, New York 2003) 133, 140-1; Giorgio Agamben, *Means without End: Notes on Politics* (University of Minnesota Press, Minneapolis 2000) 6-7.

[39] Simon (n 25) 275.

[40] Dr Maximilian Forte 'Is "Virtual" Activism Not "Real" Activism' (*Cyberspace Ethnography: Political Activism and the Internet Blog,* 29 January 2010) <http://webography.wordpress.com/2010/01/29/is-virtual-activism-not-real-activism/> accessed 20 May 2011; As Castronova has shown, even Internet role-playing games can have serious cultural and economic implications for real-world economies. See: Edward Castronova, *Synthetic Worlds: The Business and Culture of Online Games* (University of Chicago Press, Chicago 2005).

[41] Majid Yar, 'Public Perceptions and Public Opinion About Internet Crime' in Yvonne Jewkes and Majid Yar (eds), *Handbook of Internet Crime* (Willand Publishing, Devon 2010) 104-119, 106-7.

[42] Part 1. Regulating hacktivism: The focus on 'command and control'

maximise security.[43] With cybersecurity becoming a global agenda issue, hacktivism has also come to the fore, especially after the explosion of activity documented in 2011.[44]

Moreover, cyberterrorist considerations are intensified by the mass use of the medium by terrorist and extremist groups, combined with the migration of infrastructural services to cyberspace, which makes the connection between terrorist attacks and accessibility to critical resources more salient.[45] The controversial political nature and the cyberspatial interventions of hacktivism are inevitably linked to those fears and regulatory trends.[46] For example, the National Security Agency director along with other federal officials, have expressed their fears that Anonymous could soon have the ability to bring about a limited

[43] Wendy Holloway and Tony Jefferson, 'The Risk Society in an Age of Anxiety: Situating Fear of Crime' (1997) 48 The British Journal of Sociology 255*,* 260; Garland (n 24) 108-9; David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, Cambridge 2007) 16.

[44] Verizon, '2011 Was the Year of the 'Hacktivist', according to the 'Verizon 2012 Data Breach Investigations Report'' (*Verizon,* 2012) <http://newscenter.verizon.com/press-releases/verizon/2012/2011-was-the-year-of-the.html> accessed 10 November 2012; Verizon focuses, of course, more on data breaches and information thefts, rather than more symbolically expressive tactics and, thus, manage to portray hacktivism normatively as a cybersecurity threat. FBI highlighted hacktivism as a very important issue for security. Marcos Colon, 'RSA Conference 2012: Hacktivism Forcing Organizations to Look Inward' (*SC Magazine,* 29 February 2012) <http://www.scmagazine.com/rsa-conference-2012-hacktivism-forcing-organizations-to-look-inward/article/230051/> accessed 10 November 2012; Sophos security firm also named 2011 the year of the hacktivist to reflect the change in motives for cybersecurity breaches from purely criminal to more political. Sophos, 'Security Threat Report 2012' (*Sophos,* 2012) <http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/html-03.aspx> accessed 30 August 2012.

[45] McGuire (n 25) 94-5; For example, the Department of Homeland Security has defined critical infrastructure as: [T]he assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.' United States Department of Homeland Security 'What Is Critical Infrastructure?' (undated) <http://www.dhs.gov/what-critical-infrastructure> accessed 20 June 2013;
For the UK: The UK's national infrastructure is defined by the Government as: 'those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends'. Centre for the Protection of National Infrastructure 'The National Infrastructure' <http://www.cpni.gov.uk/about/cni/> accessed 20 June 2013.

[46] See Graham Meikle, 'Electronic Civil Disobedience and Symbolic Power' in Athina Karatzogianni (ed), *Cyberconflicts and Global Politics* (Routledge, London 2009) 184-5; The fear of crackdowns is also reflected in the views expressed by various activist and Internet freedom groups, who find that legal developments even from the beginning of 2000, would have a serious impact on the treatment of online activism. See The Electrohippies Collective, 'Cyberlaw UK: Civil Rights and Protest on the Internet' (*iwar.org*, 2000) <http://www.iwar.org.uk/hackers/resources/electrohippies-collective/comm-2000-12.pdf> accessed 15 February 2013; Electronic Frontier Foundation, 'Letter to Governor Pataki' (*Electronic Frontier Foundation*, 12 March 2003) <https://w2.eff.org/Privacy/TIA/20030314_letter_to_pataki.php> accessed 12 July 2012.

power outage through cyberattacks.[47] As Meikle also argues, even though acts like virtual sit-ins are exercises of symbolic power, they are portrayed as primarily coercive, which delegitimises such practices.[48]

2.2 The deviant 'Other' and hacktivists

Normative systems that are based on the existence of risks and the need to eliminate them, naturally, require a risk-provoking agent to be the deviant 'Other', against which the community will have to rally.[49] Garland characterises this process as the criminology of 'essentialised difference', which trades in archetypes and symbolisms, rather than careful research and analysis of findings.[50] Perceptions of criminality in the current era, where fear of crime has become a dominant policy-making rationale,[51] increasingly detach deviance from social causes and attribute it to the personal characteristics of a dangerous 'Other' that incorporates the dominant social fears.[52] Even though security is considered to be a general public good that all citizens should enjoy, the balancing of security against human rights often exaggerates the interests of the majority, which results in generally adversely infringing the rights of weaker and marginalised minorities.[53] Even when tolerance is advocated for some minority opinions, this is a politically-charged tolerance that presumes the approval of the minority's demands from the ruling majority, preventing any excessive challenges to the establishment.[54]

The cybercriminal archetype is the masterful and evasive hacker.[55] It presumes a highly skilled, malevolent 'super-user', functioning as the target and justification for the

[47] Andrew Couts, 'US Gov't Ramps up Anti-Anonymous Rhetoric, Warns of Power Grid Take-Down' (*Digital Trends,* 12 February 2012) <http://www.digitaltrends.com/web/us-govt-ramps-up-anti-anonymous-rhetoric-warns-of-power-grid-take-down/> accessed 20 June 2013.

[48] Meikle (n 46) 179.

[49] Holloway and Jefferson (n 43) 260.

[50] Garland (n 24) 135.

[51] Simon (n 25).

[52] Sara S. Beale, 'What's Law got to do with It? The Political, Social, Psychological and Non-Legal Factors Influencing the Development of (Federal) Criminal Law' (1997) 1 Buffalo Criminal Law Review 23, 49; Garland (n 24) 7.

[53] Lucia Zedner, 'Securing Liberty in the Face of Terror: Reflections from Criminal Justice' (2005) 32 Journal of Law and Society 507, 513.

[54] See Giovanna Borradori, *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Jacques Derrida* (University of Chicago Press, Chicago 2003) 40-1.

[55] Katja F. Aas, *Globalization & Crime* (Sage Publications Ltd, London 2007) 164, 167; Wall (n 43) 16.

broadening of the scope and intensification of strictness of cybercrime legislation.[56] Terrorist discourses have gradually also politicised this initial archetype, instituting the cyberterrorist and, to an extent the hacktivist, due to its potential association with cyberterrorism, as a contemporary ultimate threat.[57] The unpredictable hacker collective dominates cybercriminal discussions, with authorities re-labelling hackers and online activists as ‘information terrorists’, thus increasing popular condemnation for hacktivists, while legitimising stricter online controls against them.[58]

The generation and projection of the archetypal cybercriminal image currently influences how hacktivists are also perceived, since there initially appear to be many similarities between hacktivists and cyberterrorists, such as their hacker background as well as their often radical political beliefs. The negative labelling of ECD is also intensified by the size and consistency of Internet-based small hacktivist groups. Due to the pseudonymous or anonymous character of these collectives and their lacking of any specific political constituency and much offline contact with the wider public, most citizens are largely ignorant of the ideology, motives goals and tactics of these groups.[59] The maintenance of this vagueness regarding hacktivist groups facilitates the corruption of the hacktivist image and shifts the focus from contextual assessment of dangerousness and morality to homogenised perceptions of criminality that blur any moral distinction between profit-seeking cybercriminals and hacktivists who violate cybercrime laws as a means for expressing dissent online.[60] As Samuel argues, the events of 9/11 placed information security and cyberterrorism at centre stage and generally reduced tolerance towards politicised cybersecurity threats,[61] with hacktivists also documenting an increasing

[56] Ohm Paul, 'The Myth of the Superuser: Fear, Risk, and Harm Online' (2008) 41 University of California Davis Law Review 1327.

[57] Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, New York 2007) 62, 66; McGuire (n 25) 94.

[58] Kristin Finklea and Catherine Theohary,'CRS Report for Congress: Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement' (Congressional Research Service, 2013) <http://www.fas.org/sgp/crs/misc/R42547.pdf> accessed 04 May 2013; Reid Skibell, 'Cybercrime and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act' (2003) 18 Berkeley Technogy Law Journal 909, 918, 921; Majid Yar, *Cybercrime and Society* (Sage Publications Ltd, London 2006) 57; Meikle (n 46) 184-5.

[59] Skibell (n 58) 921.

[60] David M. Zlotnick, 'The War within the War on Crime: The Congressional Assault on Judicial Sentencing Discretion' (2004) 57 South Methodist University Law Review 211, 247.

[61] Alexandra W. Samuel, 'Hacktivism and the Future of Political Participation' (DPhil Thesis, Harvard University 2004) 243.

tendency of governments and e-commerce lobbyists to portray ECD as terrorist activity.[62] It should, however, be emphasised that, despite the salience of cyberterrorism as a threat, destructive incidents of cyberterrorism have yet to materialise, which highlights the exaggerated and dramatised nature of the cyberterrorist discussion.[63]

2.3 The influence of the media, experts and security firms

As has been argued previously,[64] the structuring of online norms largely relies on power networks that manage information production and distribution. Consequently, the power of mainstream media, despite the alternative channels of communication online, still dominates norm-setting. Mainstream media generate, repeat and magnify the normative messages of risk and fear in order to satisfy viewers, corporate sponsors and their stock-holders by attracting audience attention through sensationalist accounts that hopefully guarantee their viability.[65] As research has shown, the media have an ‘agenda-setting’ and ‘priming’ effect on the public in relation to crime, thus, intensifying fear and support for punitive policies.[66] Spectacular media representations also tend to overstate the role and power of technology in order to satisfy the socially pervasive technophobia.[67]

Moreover, incidents of criminality are intensely magnified by the hyper-connectivity and the ease of transferability and reproduction of news of crime through digital media (videos,

[62] DJNZ and The Action Tool Development Group of the Electrohippies Collective, 'Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?' (2001) 34 Leonardo 269, 269.

[63] Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' (2007) 97 Journal of Criminal Law & Criminology 379*,* 389; International Telecommunication Union ICT Applications and Cybersecurity Division,'Understanding Cybercrime: A Guide for Developing Countries' (International Telecommunication Union, 2009) <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf> accessed 26 January 2013, 52-3, 56.

[64] See Ch 1, Part 1.2 The modern networks.

[65] Castells, *Communication Power* (n 27) 89, 424; Beale, 'What's Law Got to Do with It?’ (n 52) 44-6; Wall (n 43) 15.

[66] Media increase the salience of certain socio-political issues by projecting these more intensely and, thus, set social agenda priorities. Subsequently, they prime audiences to believe in the increased importance of those social issues. ‘Priming’ is based on ‘cognitive accessibility’ theory, which supports that when people make judgments they employ shortcuts in the subconscious that make use of the most mentally-accessible information, being recently acquired, commonly employed or sensational. Sara S. Beale, 'The News Media's Influence on Criminal Justice Policy: How Market-Driven News Promotes Punitiveness' (2006) 48 William & Mary Law Review 397*,* 441-4.

[67] Aas (n 55) 155; McGuire (n 25) 89-90; Ranum (n 32) 135; Yar, 'Public Perceptions and Public Opinion About Internet Crime' (n 41).

photos), and thus, eventually aggravate the tendency to exaggerate risk possibilities.[68] The Internet provides access to diverse sources of information through blogs or alternative news sites that filter and tone down sensationalised and dramatised reporting and public discussion.[69] However, the majority of citizens would usually visit the traditional major media, which generally reproduce the TV-based news that the same corporate group broadcasts.[70] Although cross-posting of information in social media has allowed for the proliferation of more views, simultaneously, the capacity the Internet offers for personalised filtering and customisation of user experience neutralises this effect, with people focusing and interacting more with sources that align with their views.[71] Because the public demands quick and efficient public policies to deal with the social problems at hand, the proliferation of crime reporting online intensifies the public sense of abstract danger, infusing web-forums with 'moral panics'[72] and discursive 'cascades' that support intensified security measures.[73] Hacktivism, which has recently become a prominent cybercrime concern, will inevitably also feature in these popular discussions, making its alleged threats more salient.

Information about risk is also presumed to be structured on expert assessments that influence public perceptions.[74] Beck has argued that our social focus on risk is not because of an intensification of risk, but because our perception of risk has changed through the bombardment of the public with scientific material that magnify risk.[75] The privatisation of security alongside the intense commercialisation of the Internet, have generated an increasing interest for private corporations to support and promote security-focused discourses and regulations.[76] The focus on security serves to protect the companies' goods and investments more intensely and enable particularly security companies and experts to

[68] Sunstein, 'Laws of Fear' (n 26) 102; Aas (n 55) 155; McGuire (n 25) 116-7.

[69] Beale, 'The News Media's Influence on Criminal Justice Policy' (n 66) 437-8; Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press, London 2006) 241-2.

[70] Benkler (n 69) 245.

[71] Cass R. Sunstein, *Republic.com 2.0* (Princeton University Press, Princeton 2007).

[72] Moral panics ensue when 'a condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests' Stanley Cohen, *Folk Devils and Moral Panics* (Paladin, St Albans 1973) 9.

[73] Aas (n 55) 167; Yar, 'Public Perceptions and Public Opinion About Internet Crime' (41) 105-6.

[74] Hazel, Kemshall, *Understanding Risk in Criminal Justice* (Mike McGuire ed, Open University Press, Maidenhead 2003) 6.

[75] Deborah Lupton, 'Risk' (Taylor and Francis E-Library, 2005) 61-2.

[76] Hudson (n 25) 70.

promote their own products and services.[77] Moreover, corporate lobbying facilitates the generation and circulation of many security assessments and expert claims that often emphasise and exaggerate the potential criminal risks in cyberspace.[78]

Wall expresses doubts as to whether expert and security company assessments reflect the true extent of the risks. As he argues, reliance on experts and private security companies or self-reporting victimisation surveys can entail risks in themselves and expert knowledge is not to be followed uncritically.[79] This is because the decentralised environment, in which cybercrime thrives, undermines the reliable collection of data, since victimisation reports do not flow through a single official portal and, in fact, official sources for assessing cybercrime risks are very few.[80] Leyden, for example, has deconstructed spyware infection reports by a cybersecurity firm, demonstrating how the survey was methodologically structured in a way that greatly increased the reported number of computer compromises.[81] Consequently, the incapacity to validate expert claims that shape public opinion and governmental policies often leads to excessive reliance on traditionally inflated statistics about cybercrime that private actors will often have an interest in promoting.[82] Within such a climate, multiple security compromises that are put under the label of hacktivism end up portraying these activities as the core of dystopian cybersecurity predictions of security firms and experts.[83]

Moreover, the labelling that ensues from these cybersecurity reports marginalises the targeted citizens and induces a part of them to play into the deviant role prescribed for them.[84] the labelling of hacktivists feeds a vicious circle, where concerns for hacktivist dangerousness are sometimes further reinforced by the protesters' tactical choices and their radical and retaliatory rhetoric. Anonymous, for example, demonstrates inconsistent,

[77] Ales Zavrsnik, 'Cybercrime Definitional Challenges and Criminological Particularities' (2008) 2 Masaryk University Journal of Law & Technology 1, 4; Garland (n 24) 17.
[78] Hudson (n 25) 64; Wall (n 43) 17-8, 23-4.
[79] Wall (n 43) 13.
[80] ibid 17.
[81] John Leyden, 'Webroot Guesstimates Inflate UK Spyware Problem' (*The Register*, 20 October 2005) <http://www.theregister.co.uk/2005/10/20/webroot_uk_spyware_guesstimates/> accessed 21 April 2012.
[82] Wall (n 43) 23-4.
[83] Sophos (n 44); Verizon (n 44).
[84] Hudson (n 25) 25.

diverse behaviours, with both moral, but also often vigilantist rhetoric and tactics,[85] which can result in portraying hacktivists as potentially dangerous or immature.[86] Due to the lack of hierarchy and the anonymity that characterises many users acting under the banner of Anonymous, various radical declarations, such as an intention to shut down the Internet, have been attributed to them, only to see members of the collective dispute such aims through the online channels of communications later on.[87] Despite beliefs to the contrary, as can be seen when one examines the background and age of arrested hacktivists, many of them do not fit the typical hacker stereotype of the immature, ignorant kid, but are of varying age-groups and social backgrounds, although predominantly young.[88] Nonetheless, it is apparent that hacktivism has gradually become almost synonymous to the most important cyberthreats, with some more highly publicised immoral actions also condemning the moral ones and creating an atmosphere of general condemnation. The distorted information that proliferates in relation to the risks and dangers of cybercrime and hacktivism specifically will, in turn, have an impact on how cybercrime policy is shaped and enforced, since public views influence policies and vice versa.[89] In the UK, the Law Commission argued that the criminalisation of hacking was mainly done in order to steer the climate of opinion towards unauthorised access and not in order to punish offenders,

[85] See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism. The rhetoric of Anonymous can often be characterised as retaliatory and threatening, with videos suggesting that governments should abide by certain standards that Anonymous designate in their declaration videos in order for the group to refrain from organising protests against those targeted. Anonymous, 'Anonymous Press Release: Open Letter from Anonymous to the UK Government' (*Anonymous,* 27 January 2011) <http://.webs.com/ANONYMOUS-PRESS-RELEASE_27-01-2011.pdf> accessed 10 November 2012. In other instances, Anonymous have also publicised code of practice for protesters that are oriented towards preventing any violence and radical tactical choices and in avoiding arrests due to provocation and illegal acts. Anonymous, 'Anonymous - Code of Conduct' (*YouTube* 21 December 2010) <https://www.youtube.com/watch?v=-063clxiB8I> accessed 16 February 2013.

[86] Jana Herwig, 'Anonymous: Peering Behind the Mask' (*The Guardian,* 11 May 2011) <http://www.guardian.co.uk/technology/2011/may/11/anonymous-behind-the-mask> accessed 15 February 2013.

[87] Couts (n 47).

[88] See different age groups and different professions in Gerry Smith and Ryan J. Reilly, 'Alleged 'Paypal 14' Hackers seek Deal to Stay out of Prison after Nearly 2 Years in Limbo' (*Huffington Post,* 18 May 2013) <http://www.huffingtonpost.com/2013/05/18/paypal-14-hackers_n_3281768.html> accessed 20 May 2013.

[89] For the views that public opinion is influencing public policy, but also for the compromising of the impact of public influence by the pressures of interest groups and strong financial actors see many sources in Benjamin I. Page and Robert Y. Shapiro, 'Effects of Public Opinion on Policy' (1983) 77 The American Political Science Review 175, 175-6; As Burstein argues, although many theorists agree on the relationship between public opinion and public policy, the extent of the influence is often perceived differently. Paul Burstein, 'The Impact of Public Opinion on Public Policy: A Review and an Agenda' (2003) 56 Political Research Quarterly 29*,* 30.

demonstrating that law-making here might have initially been incongruent to the public opinion about hacking.[90]

In sum, this section has demonstrated that the general norms that dominate policy-making are predominantly oriented towards increasing the fear of crime and risk and support harsher controls in the name of security against minorities that might appear to oppose the status quo. The marginalisation of hacktivism and its labelling as a social threat would also flow from the prioritisation of security-enhancing policies at the expense of civil liberties and human rights of users. Furthermore, the prioritisation of security and the populist tendencies in law-making, trying to satisfy media-enhanced moral panics, would often mean that the positive aspects of hacktivist actions, such as their close relation to freedom of expression and privacy would be given much less attention than the potential risks hacktivists protests pose for online security. The impact of the normative environment will become even more obvious with the following description of the issues arising from cybercrime legislation.

3. The impact of cybercrime laws on hacktivism

3.1 The making of cybercrime laws

Considering the norms and policy-making trends just discussed, which have inevitably impacted and have been impacted upon by Internet-related legislation, one can see how cybercrime legislation would be a prominent regulatory tool in the processes of security norm-setting, risk-minimisation and information/network control at the hands of regulators. Indeed, as Skibbel informs us, cybercrime legislation has been a peculiar area of law that was first created as a response to public fears generated by a hacker-related movie, War Games, even before the advent of the Internet.[91] Cybercrime laws have been expanding and becoming stricter ever since, based on the consistent political support for intensification of controls of activity online and also on a general indifference of policy-makers to the practical effects of such a growing intensification of restrictions and

[90] Law Commission, ‘Computer Misuse’ (Report No.186, Hansard 1989) para.2.23.
[91] Skibell (n 58) 910.

penalties.[92] On a less critical note, Decker, argues that, consistently with the policy-making focus on risk-minimisation and prioritisation of security, the main reason for promulgating cybercrime laws has been the prevention of the increasing damages and losses that cybercrime causes.[93] Moreover, the increasing dependence of critical infrastructures, such as the electricity power grid or even banking systems on networked computing, in conjunction with the increasing concerns for cyberterrorism, have further intensified the concerns for building a robust and all-encompassing cybercriminal law structure.[94] As Moitra argues, however, cybercrime laws expand based primarily on the allegedly increasing technical capabilities of deviants, individual cases and presumptions on the actual nature of cybercrime.[95] Yet, he argues, there is little practical knowledge informing these laws in terms of the actual prevalence of certain types of cybercrime, the tactics and impact of cybercrime activities, the seriousness of these crimes, the actual victimisation that occurs, the investigative and prosecutorial procedures and the allocation of resources.[96]

How then does a cybercrime regime, which focuses on reducing risks, achieving publicisable results to allay moral panics, controlling information and promoting commercial interests, while bearing little concern for the practical reasons and consequences of its expansion and the balancing of security and rights, impact on hacktivism? The following section will discuss the existing legislation in the US[97] and the UK in relation to hacktivist tactics, such as defacements, virtual sit-ins, data thefts and will also discuss whether and to what extent the changes in law, but also the systemic problems of the cybercrime regime can have an increasingly adverse impact on hacktivism that could render the cybercriminal law regime an inappropriate tool for regulating such political activities.

[92] ibid 910-1.

[93] Charlotte Decker, 'Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime' (2007) 81 South California Law Review 959, 961.

[94] ibid 961-2.

[95] Soumyo D. Moitra, 'Developing Policies for Cybercrime-Some Empirical Issues' (2005) 13 European Journal of Crime, Criminal Law and Criminal Justice 435, 436.

[96] ibid.

[97] The analysis of US law will focus only on federal cybercrime laws, even though there is an abundance of state laws not only for reasons of brevity, but mainly because hacktivist actions usually relate to federal offences as will be seen throughout the analysis.

3.2 The applicable unauthorised access offences

In the US, the main applicable Act for hacktivist actions that has also been employed in prosecutions of hacktivists is the Computer Fraud and Abuse Act of 1986 (CFAA).[98] Since 1984 it has been amended many times, often in response to the ever–growing challenges and the socio-political influences that have gradually led to a more inclusive and harsher approach to cybercrime.[99] There are various provisions in the updated CFAA that are applicable to hacktivist actions, such as section 1030(a)(2)(C) criminalising whoever intentionally accesses a 'protected computer' without authorisation or exceeds authorised access, and thereby obtains information.[100] Section 1030(a)(2)(C) mainly incriminates hacktivists causing webpage modifications (defacements and redirects) that inevitably require unauthorised access to gain control of the webpage layout (root access) in order to modify it or modify the Universal Resource Locator (URL) of a certain page, so as to link to another critical website instead.[101] Data thefts from 'protected computers' are also prosecutable under this provision.

An important element of this offence is the expansion of its jurisdictional reach with the gradual broadening of the definition of the term 'protected computer', which seems adequate to cover most unauthorised acts targeting computers within the US and

[98] 18 U.S.C., Part I, Title 47, Section 1030 (Fraud and related activity in connection with computers) Here the commonly used name of the provision as the Computer Fraud and Abuse Act 1986 (CFAA) will be used.

[99] The most important amendments were introduced in 2001 with the PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 - USAPA) 115 Stat. 272 (2001) and Identity Theft Enforcement and Restitution Act, 122 Stat. 3560 (2008).

[100] Initially 'protected computer' was defined as a computer 'used by the federal government or a financial institution' or one 'which is used in interstate or foreign commerce'. The current, considerably broader defines a protected computer as 'a computer '(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in *or affecting* interstate or foreign commerce or communication including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.' Section 1030(e)(2).

[101] Eric Sinrod and William Reilly, 'Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws' (2000) 16 Santa Clara Computer & High Tech Law Journal 177, 212-3.

abroad.[102] The USAPA[103] made the definition of 'protected computers' inclusive of computers abroad, so long as they affect interstate or foreign commerce or communication in the United States, thus, speeding up domestic procedures relating to international offences and explicitly creating the option to prosecute US offenders attacking foreign targets.[104] The expansion of the jurisdictional applicability of the CFAA on a global scale was finalised with the Identity Theft Enforcement and Restitution Act of 2008,[105] which extended the definition of 'protected computers' to encompass, not only computers *'used in'*, but also those *'affecting'* interstate or foreign commerce or communication - in essence, every single computer online – and thus made the avoidance of US jurisdiction almost impossible for cyberdeviants globally.[106] For the UK, all Computer Misuse Act 1990 (CMA) offences must demonstrate an adequate link to the UK of either the perpetrator or the target being located in the UK.[107]

The expansion of the jurisdictional reach of the US cybercrime regime has also been facilitated by the general expansion of cybercrime legislation in many other countries along similar lines with the US,[108] which would, thus, in theory allow US prosecutors to secure extraditions of cyberdeviants abroad, based on the satisfying of the dual criminality doctrine. Considering how hacktivism is a global practice and dissent against the US could be expressed through hacktivist actions from abroad, even from countries that the US attempts to unjustly implement controversial policies, the expansion of the capacity to extradite foreign protesters can lead to the curtailment of expression of international dissent online against the US government or its corporations.

[102] Marshall Jarrett et al.,'Prosecuting Computer Crimes'(Criminal Division Computer Crime and Intellectual Property Section Criminal Division, Department of Justice, Washington D.C., undated) <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf> accessed 20 May 2011, 3-4.

[103] (n 99).

[104] Mark G. Milone, 'Hactivism: Securing the National Infrastructure' (2002) 58 The Business Lawyer 383, 390-1.

[105] (n 99).

[106] ibid, Section 207.

[107] Richard Walton, 'The Computer Misuse Act' (2006) 11 Information Security Technical Report 39, 42; see: CMA, Sections 4-5.

[108] There are many similar provisions within the European Union and the Commonwealth that could be employed to satisfy the dual criminality doctrine that is crucial for extraditions. Gregor Urbas, 'Criminalising Computer Misconduct: Some Legal and Philosophical Concerns' (2006) 14 Asia Pacific Law Review 95, 102-4; Chief Judge Stein Schjølberg, '*ITU Global Cybersecurity Agenda [GCA]*' (High Level Experts Group [HLEG] Global Strategic Report, International Telecommunications Union, Geneva 2008)< http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf> accessed 15 February 2013, 14.

In any case, the obtaining of information from a protected computer after unauthorised access was secured, which could be interpreted as just viewing the information,[109] is a misdemeanour, punishable by up to one year imprisonment and/or a fine of up to $100.000.[110] If the accessed information is further used for personal gain or other criminal purposes or the information has a value of at least $5000, this act could be considered a felony, punishable by up to five years imprisonment and/or $250.000 fine.[111] For recidivists, the penalty could go up to 10 years in prison and a $250.000 fine.[112]

Similar to 1030(a)(2), section 1030(a)(3) is also applicable to defacements/redirects, data thefts and political viruses. It criminalises the intentional, unauthorized access to 'any **non-public** computer of a department or agency of the United States or the accessing of such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;' (emphasis added) This offence is usually punishable by fine and/or a maximum penalty of one year imprisonment, while penalties for recidivists could be 10 times higher.[113]

Similar offences in the UK can be found in Sections 1 and 2 of the CMA.[114] Section 1 criminalises unauthorised access, which only demands that the computer is manipulated intentionally to perform any action in order to secure unauthorised access. The offence is now punishable by up to two years imprisonment on indictment, making it extraditable and also enabling prosecution for aiding, abetting, counselling and procuring the principal offence.[115] Additionally, section 2 of the CMA criminalises unauthorised access if it is realised with the intent to commit or facilitate the commission of a further serious

[109] United States Senate (1996) 'The National Information Infrastructure Protection Act of 1995' (Report 104-357) 6-7 cited in Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Congressional Research Service, Report for Congress, DIANE Publishing, 2011) 16.

[110] Section 1030(c)(2)(A).

[111] Section 1030(c)(2)(B).

[112] Section 1030(c)(2)(C).

[113] Sections 1030(c)(2)(A) and (c)(2)(C).

[114] (c.18).

[115] John Worthy and Martin Fanning, 'Denial-of-Service: Plugging the Legal Loopholes?' (2007) 23 Computer Law & Security Report 194, 196; Stefan Fafinski, 'The Security Ramifications of the Police and Justice Act 2006' (2007) 2 Network Security 8, 10.

offence.[116] Section 2 is a more serious offence, covering unauthorised access with a further intent to cause harm, such as stealing information to commit fraud.[117] The maximum penalty on indictment is five years imprisonment and a fine.[118] It is questionable however, whether such an offence would ever be employed against hacktivist actions, since, as will be seen in the next section, all actions of hacktivists are covered by the computer impairment offence that has been consistently employed. Furthermore, the purpose of this offence is to punish unauthorised access more seriously, when this is done with an ulterior criminal motive and not just as the plain unauthorised access. For hacktivists, the only motive would be to cause computer impairment and modification as a form of expressing dissent and therefore, ulterior criminal motives that would not be covered by the computer damage section we will analyse directly below.

3.3 The dominating provision of computer damage

Despite the applicability of unauthorised access provisions to specific hacktivist tactics, the most appropriate and all-inclusive section of the CFAA for prosecuting hacktivists is section 1030(a)(5)(A), which deals with knowingly causing a transmission of a program, information, code or command which results in intentionally causing damage without authorisation to a 'protected computer'. Moreover, two additional offences are included, which deal with intentional unauthorised access to a protected computer that results in reckless damage, Section 1030(a)(5)(B) or damage and loss, Section 1030(a)(5)(C).

Damage is limited to economic damage and this is defined in Section 1030(e)(8) as 'any impairment to the integrity or availability of data, a program, a system, or information'. Most hacktivist tactics, which manipulate, impair, suppress access and availability of information or compromise the integrity of websites and even servers, would generally fit this description.[119] Moreover, loss is defined as: 'any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and

[116] CMA Section 2: This section applies to offences:
a. for which the sentence is fixed by law; or
b. for which a person of 21 years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980 (c.43).

[117] Walton (n 107) 41.

[118] Section 2(5).

[119] Marshall Jarrett et al. (n 102) 34-7.

restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.'[120]

The analogous UK provision is Section 3 of the CMA providing that whoever knowingly performs any unauthorised act in relation to a computer with the intention to impair the operation of any computer, prevent or hinder access to any program or data held in any computer, impair the operation of programs or reliability of data or enable the above actions[121] could incur penalties of imprisonment of up to ten years and/or fine on indictment, while up to a year and/or fine on a summary conviction (6 months in Scotland).[122] Section 3(3) also broadens the scope of the offence by criminalising recklessness of the offender regarding the realisation of the above impairing/damaging effects.

There are three major issues with the computer damage provisions that have an impact on hacktivism. The first is the issue of very high potential penalties that are linked to vague and arbitrary definitions and assessments of damage and loss. Moreover, this increased focus and broadening of the scope of damage and loss is further exacerbated by the inclusion of easily satisfiable criteria for activating felonious charges in the CFAA that are also linked to damage and loss. The second issue relates to the vagueness in relation to unauthorised access and the intent to cause damage. The third is the ease with which computer damage offences could be linked to cyberterrorism and the impact this could have on punishment ranges and also the monitoring and labelling of protesters. Although these issues relate predominantly to the US, UK provisions also demonstrate similar, yet not as intense, problems and will be discussed in parallel, where appropriate.

3.3.1 The focus on damage and loss and the expansion of the scope

The US cybercrime regime has become increasingly stricter over the years, with higher penalties, lower standards for felonious liability, broader criminalisation of reckless or negligent mens rea and mainly an intense focus on damage and loss, rather than moral culpability.

[120] Section 1030(e)(11).
[121] Sections 1030(3)(2) (a-d).
[122] Sections 1030(3)(6)(a-c).

Defining and calculating damage and loss is a very thorny issue, as the broadness with which they are defined can often lead to very high assessments amounting to analogously high penalties.[123] For example, after 2001 in the US, in addition to eliminating the need to prove intent for causing a specific amount of loss, courts have gradually extended the range of types of losses that could be calculated in order to assess the felonious character of the offences and the extent of the penalties.[124] Even in cases, where protesters might take precautions to minimise damages, prosecutors can thus include various unforeseeable damages/losses in their assessment, which will eventually increase potential sanctions. US courts have also exacerbated the tendency to accommodate victims, having often accepted with little challenge the victims' damage and loss assessments.[125]

Moreover, the US Sentencing Guidelines have recently included pecuniary losses that do not even have to satisfy the criterion of reasonable predictability.[126] They also distinguish penalty ranges based mainly on economic criteria, and they disregard instrumental concerns in relation to potential benefits from benign hacking.[127] Mitigating factors are much less explicit and less numerous than aggravating factors, which are by contrast explicitly detailed.[128] Finally, the CFAA contains a civil suit provision that can also be

[123] Jarrett et al. (n 102) 34-5.

[124] ibid 37-9; Reasonable costs to any victim, include the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; Section 1030(e)(11); This definition could include the prorated salary of system administrators, the wage of web-security personnel, the expense of re-creating lost work, the cost of re-installing system software and security measures. See: *US v. Middleton* 231 F.3d 1207 (9th Cir. 2000); *EF Cultural Travel BV v Explorica, Inc* 274 F.3d 577 (1st Cir. 2001); Loss could also include harms like lost advertising revenue or sales and the salaries of employees who are prevented from working due to systems inoperability. Jarrett et al. (n 102) 40.

[125] Skibell (n 58) 930-4; See U.S.S.G. (n 142) Section 2B1.1(b)(1).

[126] See The commentary to the 2008 Guidelines it is stated that 'actual loss *includes* the following pecuniary harm, *regardless of whether such pecuniary harm was reasonably foreseeable:* any reasonable cost to the victim including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.' See United States Sentencing Commission, 'United States Sentencing Guidelines' (2008) Section 2B1.1, cmt. n.3(A)(v)(III) cited in Jarrett et al. (n 102) 111.

[127] Anonymous, 'Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm' (2006) 119 Harvard Law Review 2442, 2453-4; Considering how Paypal claimed losses of $5.5 million from operation Payback, it would not be surprising to have such great increases in sentences for protesters on the basis of their attacks having compromised the financial security of those companies.

[128] U.S.S.G. (n 142) Chapters 2 and 3. Perhaps one of the most characteristic examples of the focus of the orientation of the Sentencing Guidelines is the potential increase of 18 degrees in the punishment scale for a computer damage attack that could threaten the financial security of a

brought against those criminally charged for restitution, making the ultimate penalty even higher.[129] Consequently, the calculating philosophy that permeates cybercrime legislation and sentencing guidelines renders the current cybercrime regime inappropriate to deal with hacktivism, particularly in producing tolerance and proportionate penalties, something which would interest those amicably oriented towards hacktivists.

The dominant economic orientation of the computer damage provisions not only compromises the attribution of deserved punishment, but also leads to less principled types of protest since the preservation of moral safeguards when protesting seems to have very little mitigating impact in the current structure of liability processes, especially since damage and loss assessments easily reach high amounts, which in turn make tactical efforts to minimise damage or loss seem almost counterintuitive. Consequently, the lack of tolerance and proportionate penalties often lead to more numerous and radicalised protests, thus,[130] rendering the use of rigid cyberlaws a problematic tool even for those desiring the reduction of hacktivism.

For the CFAA, current penalties can reach up to ten years imprisonment for first time offenders for even attempts to commit the 1030(a)(5)(A) (intentional damage) offence, or five years for causing reckless damage 1030(a)(5)(B), if one of the harms included in the sub-clauses (I) to (VI) of section 1030(c)(4)(A)(i) are satisfied.[131] Even when the triggers defining felonious damage are not satisfied though, the penalties are high, since for first time offenders computer damage of any kind could mean up to one year in prison and a fine of up to $100.000, whereas penalties could rise up to 20 years and a fine of $250.000 for recidivists causing non-serious damage intentionally (1030(a)(5)(A) or recklessly (1030(a)(5)(B)) and up to 10 years for violation of (1030(a)(5)(C)).[132] Since many ECD protesters will usually be involved in more than one protest, the high recidivist penalties

publicly traded company or one with more than a 1000 employees, a type of target that is very commonly the target of hacktivist protests. See U.S.S.G. (n 142) Section 2B1.1.15B. The increase would be translated to an increase from 0-6 months to 51-63 months of imprisonment. Considering how Paypal claimed losses of $5.5 million from the operation Payback, it would not be surprising to have such great increases in sentences for protesters on the basis of their attacks having compromised the financial security of those companies.

[129] Section 1030 (g).

[130] See also discussion in Ch 3, Parts 2.2.3 Are highly punitive sanctions for ECD utilitarian? and 3.3.2 Communication theory, punishment and ECD.

[131] Section 1030(c)(4)(B)(i) and (ii); Indicative of the harshness of these penalties is the fact that they maximum is equal to that of voluntary manslaughter. See: U.S.C. Title 18 Chapter 1112.

[132] Sections 1030(c)(4)(A), (c)(4)(D), (c)(4)(G).

could eventually become applicable, if convicted hacktivists participate in future protests. Moreover, consecutive prosecutions become even more probable when one considers that, under normal circumstances, easily identifiable hacktivists protesting openly could be prosecuted more easily that anonymous, skilled cybercriminals, which are the primary targets of cybercrime legislation.[133]

In addition to the increasingly high penalties in general, the CFAA felony triggers were amended to include low damage/loss requirements that can be satisfied even by minor criminal acts, such as those often perpetrated by hacktivists. Not all triggers are applicable to hacktivist tactics, so the focus here will be only on the relevant ones. The harms that trigger felonious liability – also requiring the causing of some amount of damage - are:

> (I) loss to one or more persons during any one-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only; loss resulting from a related course of conduct affecting one or more other protected computers) aggregating at least $5,000 in value[134]; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security;[135] (VI) or damage affecting 10 or more protected computers during any 1-year period.[136]

The more directly and generally applicable are triggers (I) and (VI). Starting with trigger (I), after 2001, the need to prove intent to cause $5000 of loss was eliminated and prosecutors are only required to prove intent to cause damage.[137] Moreover, despite the already broad definition of loss,[138] the types of loss included are not deemed exclusive and assessments can include additional types of financial setbacks, which are unlisted.[139] The easily satisfiable expectation that simply relates to causing only some amount of damage, in

[133] Ohm (n 56).

[134] Section 1030(c)(4)(A)(i)(I).

[135] Section 1030(c)(4)(A)(i)(V).

[136] Section 1030(c)(4)(A)(i)(VI) Harms that relate to meddling with medical records and causing of physical injury and threat to public health or safety are also included but will not bother us, since hacktivists, as we have seen in chapter one, avoid protesting against such sensitive targets. See also Sections 1030(c)(4)(A)(i)(I-VII).

[137] Jarrett et al. (n 102) 37-9.

[138] Reasonable costs to any victim, include the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; Sections 1030(e)(11).

[139] Section 1030(e)(11) See (n 124).

addition to the multiple elements that can be calculated as damage and loss could result in simple web-defacements or very temporarily disruptive virtual sit-ins easily exceeding the $5000 felony-triggering limit, especially for commercial websites. For example, Paypal conceded in relation to the Anonymous protests in late 2010, that there was no actual damage and disruption of services was restricted,[140] yet still protesters were prosecuted for losses of up to $5.5 million.[141]

The other two felony triggers are even more straightforward. First, virtual sit-ins and viruses could easily satisfy the 'damage to ten or more computers' requirement, especially since no specification on the amount of damage exists again. Consequently, even if one commits $1 of damage on every computer out of ten, her action could trigger felonious liability.[142] Moreover, ECD protests against computers that are used in the furtherance of administration of justice or national security could also be a very realistic possibility for triggering felonious liability for hacktivist actions, since this broad term could definitely include websites that protesters target, such as those of the Departments of Justice or other military or police websites.[143]

Although the US example is far more extreme in its focus on damage and loss, there are some aspects of the relevant UK laws that indicate a similar turn towards stricter, loss-based assessments of punishment. In the UK, the 2006 amendments to the CMA 1990 UK provisions followed the US example, doubling the penalties for computer crimes[144] and extending the scope of liability, criminalising reckless in addition to intentional impairment caused by an unauthorised act.[145] Furthermore, liability can be incurred irrespective of the duration of the impairment or the extent of damage caused, even though the EU Framework Decision (Art.3)[146] suggests that minor system interferences should not be

[140] PayPal 'Update on Paypal Site Status' (*The PayPal blog,* 09 December 2010) <https://www.thepaypalblog.com/2010/12/update-on-paypal-site-status/> accessed 09 September 2012.
[141] Josh Halliday 'Anonymous Hackers Jailed for Cyber Attacks' (*The Guardian,* 24 January 2013)<http://www.guardian.co.uk/technology/2013/jan/24/anonymous-hackers-jailed-cyber attacks> accessed 18 June 2013.
[142] See United States Sentencing Commission, '2011 Federal Sentencing Guidelines Manual ' (United States Sentencing Commission 2011) <http://www.ussc.gov/> accessed 24 February 2013(U.S.S.G.) Section 2B1.1(b)(1).
[143] Jarrett et al. (n 102) 43.
[144] See CMA 1990, Sections 1(3), 2(5), (3)6.
[145] Section 3(3).
[146] EU Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (Framework Decision).

criminalised.[147] Moreover, both the Council of Europe Cybercrime Convention[148] (Arts 4-5) and the Framework Decision (Art.3) suggest that only the intentional and serious hindering or interruption of the functionality of computer systems or data should be criminalised. However, the term 'serious' does not feature in the UK Act regarding the criminalising of illegal interference, in addition to recklessness being included as culpable mens rea, despite the guidance explicitly arguing for the criminalisation of only intentional interference.[149] As MacEwan argues, the extension of liability to reckless impairment could increase vagueness and lead to questionable prosecutions, especially since the addition of recklessness had also not been suggested by the Convention or the Framework Decision and was inserted at a stage, where it did not allow for public scrutiny.[150]

Furthermore, the UK Sentencing Guidelines,[151] which must be followed by the courts,[152] also demonstrate the importance given to culpability, the limits of which have been extended, but also to foreseeable harms, which can include loss assessments.[153] More particularly, Section 143(1) of the UK Criminal Justice Act 2003[154] clarifies that seriousness should be assessed based not only on already caused harms, but also any intended or foreseeable harms. However, it is provided that assessments should be tempered by the level of culpability, which would be determined by the nature of motives, the premeditation or spontaneity of the act or the existence of a relationship of trust between the victim and offender.[155] Despite the tempering of harm assessments by elements of culpability, it is also provided by the Guidelines on Seriousness (Section 1(11)) that, where no actual harm has occurred, courts will assess the relative dangerousness of the offender's

[147] Ian J. Lloyd, *Information Technology Law* (6th edn Oxford University Press, Oxford 2011) 234; See Section 3(5)(c).

[148] Council of Europe, 'Convention on Cybercrime' (ETS No. 185, Budapest, 2001)(Cybercrime Convention).

[149] Neil MacEwan, 'The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its Future' (2008) 12 Criminal Law Review 955*,* 964.

[150] ibid 964.

[151] Sentencing Guidelines Council, 'Sentencing Guidelines' <http://sentencingcouncil.judiciary.gov.uk/guidelines/guidelines-to-download.htm> accessed 15 February 2013

[152] Criminal Justice Act 2003, c.44, Section 170(9).

[153] Sentencing Guidelines Council, 'Overarching Principles: Seriousness' (2004)< http://sentencingcouncil.judiciary.gov.uk/docs/web_seriousness_guideline.pdf> accessed 15 February 2013.

[154] (c.44).

[155] ibid.

conduct in relation to the likelihood of harm occurring and the gravity of the potential harm.[156]

In sum, the recent addition of recklessness, both in the US and UK, could severely punish multi-actor activities, since it would be very difficult to assess, under a subjective test of recklessness, whether protesters could foresee the level of disruption of their protests and whether they would be aware of the risk of potentially enhanced harmfulness through the addition of hackers, which could contribute thousands of compromised computers to the protest.[157] Naturally, the changes that expand the liable culpability and harmfulness, such as the criminalisation of reckless damage, even in the form of short-lived, minor disruptions, essentially enable the criminalisation and serious punishment of minor offences. Reliance on assessments of potential harms and their gravity within the existing security-focused climate could mean that assessments of hypothetical harms could seriously impact on the extent of punishment assessments of individuals that participate in activities, the potential harms of which, would be very hard to gauge based on the stakeholders' potentially conflicting hypotheses.

3.3.2 The further criminalisation of inchoate offences

The chance for potential felonious liability in the US is even more increased, since the scope of inchoate offences, such as attempt, incitement and conspiracy charges and their punishment, have increased accordingly, being punishable as consummated offences.[158] Especially conspiracy was only added in 2008 with the Identity Theft Enforcement and Restitution Act 2008.[159] Similarly in the UK, all offences can now be prosecuted for aiding or procuring the principal offence, incurring penalties at the level of a consummate offence, even for just divulging information on computer weaknesses and even orally offering advice on how to participate in a virtual sit-in.[160] For example, enablement of unauthorised access (Sections 1(a) and (b)) and computer impairment (Section 3(2)(d)) were explicitly added with the Police and Justice Act of 2006. Furthermore, hacktivists have been charged with

[156] ibid.

[157] As Lord Bingham stated in *R v G and Another* [2003] UKHL 50:
' a person acts 'recklessly' with respect to: (i) a circumstance when he is aware of a risk that it exists or will exist; (ii) a result when he is aware of a risk that it will occur; and it is, in the circumstances *known to him*, unreasonable to take the risk.'

[158] See Sections 1030(b) and (c).

[159] Section 206.

[160] Fafinski, 'The Security Ramifications of the Police and Justice Act 2006' (115) 10.

conspiracy to impair a computer network based on section (1)(1) the Criminal Law Act 1977,[161] while section (1A) of the same Act could also be used to criminalise conspiracies outside England and Wales, as amended by the Coroners and Justice Act of 2009.[162] The increasing criminalisation of inchoate offences, generates even more complicated scenarios for hacktivists since even failed or weak virtual sit-in attempts, could be prosecuted and have indeed, been prosecuted as conspiracy offences both in the US and the UK, thus, increasing the potential penalties.[163] Naturally, if hacktions are considered terrorist,[164] hacktivists who even incite such protests could also be prosecuted for several inchoate offences like public provocation or recruitment.[165]

In relation to aiding, the production and distribution of hacking tools is not included in the CFAA. Section (a)(6) only discusses trafficking in passwords and information enabling unauthorised access with the purpose of committing fraud. The production and trafficking of unauthorised access devices[166] is also considered an aggravating factor for cybercrime offences in the US Sentencing Guidelines.[167] The applicability of Section (a)(6) to hacktivist software, however, is unclear since prosecutors need to also prove a purpose to defraud and, as has been discussed throughout the thesis, hacktivists violate cybercrime laws for symbolic, political reasons, even if misguided sometimes, and not for making money out of unsuspecting users or companies. Whether virtual sit-in tools could be considered unauthorised access devices is also arguable, depending on the conception adopted regarding the lack of authorisation in virtual sit-ins. However, such a prospect seems far-fetched.

On the contrary, the UK has explicitly criminalised the production and distribution of articles that facilitate unauthorised access and impairment. Section 3A of the CMA 1990

[161] (c.45)

[162] Section 72.

[163] See David Kravets 'Virtual Sit-Ins Doom Online Animal Rights Activists' (*Threat Level*, 16 October 2009). <http://www.wired.com/threatlevel/2009/10/animals/> accessed 20 May 2011 See also: *Us V Fullmer* 584 F.3d 132 (3rd Cir. 2009).

[164] Part 3.3.4 Hacktivism and the link with cyberterrorism.

[165] Schjølberg (n 108) 26-8. See Part 3.3.4 Hacktivism and the link with cyberterrorism.

[166] 'Any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.' 18 U.S.C. Part I, Chapter 47 Section 1029 (Fraud and related activity in connection with access devices) Section 1029(e)(1).

[167] See Section 2B1.1(b)(10).

criminalises the making, supplying or obtaining of articles for use in offences under sections 1 or 3 of the CMA.[168] It provides that a person is guilty of an offence if he makes, adapts, supplies or offers to supply any article (including any program or data held in electronic form) intending it to be used or believing it is likely to be used to commit or assist in the commission of offences under section 1 to 3 of the CMA 1990. It even criminalises obtaining such an article with a view to its being supplied for the above reasons, with penalties reaching two years imprisonment.

This provision requires that the perpetrator has a double intent, both to supply the article and to intend it, or believe it is likely, to be used for computer misuse offences. The proving of the second part of intent and the vagueness of the term 'likely', the interpretation of which has been left to the discretion of the courts, have caused great controversy amongst politicians, cybersecurity firms, software vendors and network operators.[169] The main reason is that the criminalisation of the ownership or sale and use of such tools without providing any legitimate use defence, as the Cybercrime Convention had advised,[170] could potentially incriminate many legitimate users, creators and sellers of such software for network security purposes.[171] This provision could further criminalise hacktivists that generate and openly distribute software, such as the Goolag scanner tool for finding technical security holes on websites, or Floodnet for facilitating virtual sit-ins.[172]

3.3.3 Unauthorised access and intentional damage

The issue of lacking and exceeding authorisation is one of the most contested in relation to cybercrime laws, creating serious ambiguities and the CFAA is the most characteristic case regarding lack of clarity of the issue of authorisation, which can seriously impact on the criminalisation of hacktivist actions. The first question to be asked before we proceed to

[168] Section 3A was introduced by Section 37 of the PJA 2006, in order to incorporate into UK law the Framework Decision (n 146).

[169] Stefan Fafinski, 'Computer Misuse: The Implications of the Police and Justice Act 2006' (2008) 72 Journal of Criminal Law 53, 60-2.

[170] Cybercrime Convention (n 148) Art.6.2.

[171] Peter Sommer, 'Criminalising Hacking Tools' (2006) 3 Digital Investigation 68, 71; The wide scope of the provision, and especially, art. 6.2, has led Bainbridge to propose that the 'likelihood' of criminal use of the article might be construed as an objective criterion founded on the belief of a similarly knowledgeable, reasonable person; David I. Bainbridge, *Introduction to Information Technology Law* (6th edn Pearson Education Limited, Essex 2007) 463.

[172] See Ch 1, Part 2.2 Hacktivist groups and tactics.

discuss the issue of authorisation is whether the intentional computer damage provision of the CFAA, section 1030(a)(5)(A) requires the act causing the damage (the transmission of information, code etc) to be unauthorised in addition to the damage being unauthorised. Considering the previous versions of this offence, the lack of authorisation was linked to the accessing act and not just to the damage.[173] One issue that comes up here is whether the transmission of information can be also considered access, so that we can then discuss whether this access is unauthorised or not. According to the most commonly used interpretation of access, it can indeed be identical to what the provision describes as the transmission of data, as simple as requesting information from a public webpage, much like how virtual sit-in protesters do.[174] In order for the provision to apply to those having authorisation to access a computer or network and still cause damage to it, the dominant interpretation of access should thus encompass the transmission of information to a website or computer network. Therefore, the lack of authorisation for the current CFAA intentional computer damage provision should be considered relevant not only to the damage, but also to the transmission that causes the damage (access).

One could argue that, for users having some degree of authorisation to access the computer or network anyway, the damage will be unauthorised, if the knowing act of transmission is unauthorised or if the transmission exceeds the level of authorisation given. After all, a damaging act would always be unauthorised for outsiders or exceeding authorisation for insiders, such as employees, since, if an act is within the authorisation given, it would constitute part of the normal duties of modification or deletion or network security assessment and would, thus, be non-damaging in the criminal sense. Therefore, the term ‘without authorization’ in Section 1030(a)(5)(A) should relate to the actual act of transmission of code that brings about the damage and not just to the damage. Keeping this initial ambiguity in mind, let us proceed to discuss how the vagueness surrounding the interpretations of ‘exceeding authorisation’ can seriously impact on hacktivists.

[173] See Doyle (109) 29; ‘Even under an earlier version of the section 1030(a)(5) that outlawed “intentional access ... without authorization, and by means of ... such conduct ... prevent[ing] authorized use of any such computer ... and thereby causes loss to one or more others of a value aggregating $1,000 or more ...,”’ *Us v Morris* 928 F.2d 504 (2nd Cir. 1991) 504 (*Morris*).

[174] See Orin S. Kerr, 'Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes', (2003) 78 New York University Law Review 1596, 1620-1. The concept of access as the exchange of information in the form of communication between two computers, rather than as intrusion into a protected virtual space is consistent with how the case law has perceived access, as will be seen below.

A case that has set an important precedent on the issue of lacking or exceeding authorisation for insiders (exceeding authorised access) is the case of *US v Czubinski*.[175] In the course of his work for the Internal Revenue Service (IRS), Czubinski was authorised to access information in the IRS computer systems, using a password given to him by IRS that allowed him to access information of tax-payers.[176] IRS rules provided that employees authorised to access the IRS computer systems were not permitted to access the files held in those databases for reasons other than performing their official duties.[177] During his employment, Czubinski conducted many unauthorised searches, knowingly disregarding the rules and looking at confidential information that was not related to his official IRS duties, out of curiosity.[178] The evidence showed no further use had been made of that information access without authorisation.[179] Czubinski remained in employment until he was indicted in 1995 by a grand jury on many counts, four of which are of interest here, as they relate to federal computer fraud under the CFAA 1030(a)(4). Since our topic is authorisation we will only assess the CFAA aspect of the case.[180]

At the time, the wording of the computer fraud provision was: 'whoever [...] knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer.'[181] The appellate court verified that Czubinski 'unquestionably exceeded authorized access to a federal interest computer',[182] based on the fact that he had used his authorisation to access that information, out of personal curiosity and not for his official duties. Consequently, authorisation to access can be exceeded, if the use of the information one is allowed to access is beyond the intended use for which authorisation was actually given. The case of intrusive protests, such as defacements, redirects and data thefts would obviously be unauthorised, as they would be perpetrated by externals that lack authorisation per se and bypass access controls. But the case of virtual sit-ins can be more complicated.

[175] *US v Czubinski*, 106 F. 3d 1069 (1st Cir. 1997)(*Czubinski*).
[176] ibid 1071.
[177] ibid.
[178] ibid 1071-2.
[179] ibid 1072.
[180] ibid.
[181] Cited in ibid 1078.
[182] ibid.

On the basis of the 'intended use' test described in *Czubinski*, virtual sit-ins would be exceeding authorisation as they would be exceeding the anticipated use for which authorisation to access a publicly accessible website is considered given for reasons of normal use of exchanging information, such as browsing or making financial transactions. Consequently, sit-ins that impair the functionality of a website go beyond what would be authorised by the website owner and inconsistent with the purpose authorisation is usually given in the first place. Therefore, virtual sit-ins according to the 'intended function' test would be acts that exceed authorisation.

This interpretation is also consistent with the rationale the court followed *in EF Cultural Travel BV v Explorica Inc,*[183] where it was decided that employing software which automates data-collection (Scraper) when accessing a public website in order to collect data, for which manual access and collection is authorised, would be exceeding the use for which authorisation was given, since the design and use of the automated search software also violated a confidentiality/non-competition agreement signed between the plaintiff and the CEO of the defendant. Although the appellate court focused more on the violation of the confidentiality agreement for establishing the exceeding of authorisation, it also seemed to accept the district court's view that the appellants had exceeded authorised access, since the use of the automated Scraper software for competitive reasons went beyond the reasonable expectations of use that would be authorised by the website owner and its users.[184] The rationale adopted in *Explorica* further defines all the elements of 'exceeding authorised access' to publicly accessible websites and also has direct applicability to virtual sit-ins. Consequently, according to *Explorica,* the way in which virtual sit-ins are often perpetrated through automated reloading software tools, (e.g. Floodnet) exceeds the use for which authorisation to access the website was given, as it goes beyond the reasonable expectations of the owners and other users, even if access to the webpage and manual reloading of it is considered authorised.

It would have to be noted here that cases of unintended use of employer information by employees have also been interpreted as eliminating authorisation, rather than exceeding

[183] *Explorica* (n 124).

[184] ibid 581-2; It is also established from the above that access is defined as the transmission of code (the Scraper software) to the publicly accessible website of the plaintiff in order to assess the exceeding of authorisation to access.

it.[185] However these cases have been criticised by recent case-law and are unlikely to be followed, especially for the cases that are of interest here relating to access to a public website with no employment relation establishing the authorisation given.[186] Therefore, I will focus on the above *Czubinski/Explorica* interpretation and will also try to show how later cases have impacted on this interpretation of exceeding authorisation and the link to the computer damage provision.

Summing up the discussion of authorisation so far, virtual sit-ins would seem covered by the *Czubinski/Explorica* rationale of exceeding authorisation, when the prosecution is based on the intentional causing of damage without authorisation. Exceeding authorisation, however, is not applicable to the CFAA's provisions that require proof of unauthorised access that causes reckless damage or plain damage and loss,[187] which were only meant to apply to external users with no authorisation whatsoever.[188] Therefore, damage caused by users having some authorisation in the first place - such as the authorisation a user has to access the main page of a publicly accessible website - can only lead to criminal charges, if the damage caused is intended. This would mean that, for virtual sit-ins, it would have to be proven that the damage to the protested website was intentional.

However, participants of virtual sit-ins have agreed to guilty plea agreements on charges of reckless damage or negligent damage and loss.[189] These prosecutions could mean two

[185] *Shurgard Storage Centers, Inc. v Safeguard Self Storage, Inc* 119 F.Supp.2d 1121 (Dist. Court, Washington D.C. 2000)(*Shurgard*) follows the termination of authorisation of employees, when their motives for accessing information contradict those of the authorising employer. *International Airport Centers, Llc v Citrin,* 440 F.3d 418 (7th Cir. 2006)(*Citrin*) also adopts the elimination of authorisation approach based on the common law of agency, since the violation of the duty of loyalty of the employee towards the employer terminates their relationship and, consequently, the authorisation of access based on that relationship.

[186] See Jarrett et al. (n 102) 6-7; The court in *US v Nosal* 676 F.3d 854 (9th Cir. 2012)(*Nosal)* and *LVRC Holdings v Brekka*, 518 F.3d 1127 (9th Cir. 2009)(*Brekka)* are clear about the fact that, if there initially exists some authorisation, then any case of going beyond the limits of that authorisation, is exceeding authorised access and not unauthorised access, as 'unauthorised' per se relates to no rights to access in the first place.

[187] Sections 1030(a)(5)(B) and (a)(5)(C).

[188] U.S. Senate Report 104-357 (n 109) 11:'In sum under the bill, insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to a computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass') cited in *US v Phillips*, 477 F.3d 215, 219 (5th Cir. 2007).

[189] *US v Guzner* No. 2:09-cr-00087 (New Jersey Dist. Court)(*Guzner*); Anonymous 'Teenage Hacker Admits Scientology Cyber-Attack USA V. Guzner – Information' (*Secretdox,* 18 October 2008) <http://secretdox.wordpress.com/2008/10/18/usa-v-guzner-plea-agreement-for-defendant-dmitriy-

different things. First, they could be demonstrative of prosecutorial disregard of legislative intentions regarding the exclusion of reckless or negligent computer damage charges for users with some degree of authorisation. Second, such prosecutions could be interpreted as denying the existence of a prima facie authorisation of users to send information requests to a publicly accessible website. In both instances there seem to be inconsistencies. In the first possible scenario, the prosecutor is trying to support a prosecution which, especially in the case of Mettenbrink who plead guilty only to negligent damage and loss, should have failed. This is because Mettenbrink had participated in a virtual sit-in that exceeded authorisation by automatically reloading a publicly accessible webpage and it was not a case of unauthorised access per se, since the transmission of data to the website that suffered the damage, and thus Mettenbrink's transmission/access, was authorised. Since intention to cause damage is required for liability to attach against those having some form of authorisation, the prosecution seems problematic.

In the second possible scenario, the prosecutor would have us accept that the existence of a publicly accessible website does not mean that we are automatically authorised to access it by transmitting information to it. There seems to be a serious interpretive vagueness here that prosecutors either chose to misinterpret or bypass altogether, perceiving access very narrowly as intrusion only, thus contradicting usual interpretations of access in case-law[190] in order to achieve guilty pleas based on the lack of clarity regarding authorisation. In any case, the vagueness regarding the concept of authorisation has led to prosecutions that further contradict the apparent legislative desires that explicitly wanted prosecutions for reckless and negligent damage to focus on users totally lacking

guzner/> accessed 20 May 2011; See also *US v Mettenbrink* Case 2:09-cr-01149-GAF (Dist. Court, California 2010)(*Mettenbrink*); David Kravets 'Guilty Plea in 'Anonymous' DDoS Scientology Attack' (*Threat Level,* 26 January 2010) <http://www.wired.com/threatlevel/2010/01/guilty-plea-in-scientology-ddos-attack/> accessed 20 May 2011; In the case of Mettenbrink, the protester is charged with negligent damage and loss, while in the former Guzner is charged with intentional damage. Both received one year imprisonment amongst other sanctions (probation, restitution, community service) which for Mettenbrink was the maximum, while for Guzner the maximum statutory penalty was 10 years.

[190] *State v Allen,* 917 P.2d 848 (Kan. 1996) has supported the view that access requires intrusion in addition to sending information requests to a website, such as bypassing a password prompt page, but the case has been superseded by other cases and did not relate to publicly accessible websites. See *America Online v. National Health Care Discount, Inc.* 121 F. Supp. 2d 1255 (N.D. Iowa 2000) and *Register.com, Inc. v Verio, Inc* 126 F.Supp. 2d 238, 255 (S.D.N.Y. 2000) where the courts adopted the broader interpretation of access as making an initial attempt to communicate by sending information requests to a website.

authorisation.[191] This demonstrates how the current cybercrime regime with all its vagueness and challenged interpretations of basic terms can be a dangerous tool for dealing with hacktivists, as it allows prosecutors to contest the will and the purposes of the legislators with their prosecutorial decisions, which, as will be seen,[192] are already wide and largely unreviewable, especially in the US.

To make matters more complicated, the court in the recent case of *US v Nosal*,[193] argued that employer-employee and company-consumer relationships, both based on private agreements, are usually regulated by tort and contract law and that the *Czubinski/Explorica* 'intended use' test would result in these relationships being manipulated by private parties in order to police them through criminal law.[194] More particularly, the *Nosal* court expressed its concern that attaching felonious liability for the CFAA on the violation of vague and unknown or arbitrarily changeable Terms of Service could criminalise millions of plain users bypassing private contracts or terms and conditions of websites. As the court further argued, despite governmental assurances that prosecutors would not resort to prosecuting superficial cases of exceeding authorisation, the current interpretation of exceeding authorisation, (*Czubinski/Explorica)* cannot be allowed as it would force citizens to greatly rely on the discretion of the prosecutors for avoiding excessive prosecutions.[195] The court further dared Congress to explicitly dictate if it wanted such cases included, since the rule of lenity requires that penal laws are interpreted strictly.[196]

This conclusion of *Nosal* regarding authorisation could mean that the criminalisation of virtual sit-ins as damaging acts exceeding authorisation - the basis of criminalisation being the unintended use of the authorisation to access a public website for impairing protest purposes - would be unsupportable, as there would be no lack or exceeding of authorisation if *Nosal* is followed. Considering that protesters merely employ their browsers to access a webpage repeatedly, without bypassing any technical restrictions,

[191] See (n 188); Sections 1030(a)(5)(A)(ii) and (iii) require proof that the defendant intentionally accessed a protected computer without authorization. These subsections do not include the phrase 'exceeds authorized access.' Thus, these subsections do not apply to authorized users of a computer who exceed their authorization (insiders).' Jarrett et al. (n 102) 36.

[192] See Part 5.1.1 Prosecutorial power and the new mentality.

[193] *Nosal* (n 186).

[194] ibid 3867.

[195] ibid 3869-70.

[196] ibid 3871-2.

according to the rationale adopted in *Nosal,* where exceeding authorisation can only be established by violating technological restrictions, the protesters sit-ins would not be exceeding authorisation. Consequently, even if they are intentionally causing damage, the *Nosal* interpretation to exceeding authorisation would support the authorised character of their acts, thus, conflicting with the element of 'without authorisation', especially if the lack of authorisation applies both to the act of transmission and the damage, as I have discussed at the beginning of this subsection. If one attempted to apply the standard of *Nosal* to virtual sit-ins, where authorisation to access (transmit information requests) the website and reload the page is considered a given due to the public accessibility of the webpage in question, the act of reloading a webpage could be considered authorised, even if the terms of use of a website prohibit the access through automating tools, such as Floodnet. Therefore, such acts of reloading would be non-prosecutable by any of the computer damage 1030(a)(5) offences. That is, of course, if we accept that, as mentioned above,[197] the intention to link the lack of authorisation to the act causing the damage, in addition to the damage per se, has been preserved in the CFAA current computer damage provision.

Botnet-enhanced denial of service attacks (and virtual sit-ins) would still, of course, be criminalised, since the use of botnets would be unauthorised, as their hacker-controller will have bypassed technical restrictions in order to gain control of the computers constituting the botnet and will be using them to attack the targeted website against their owners' volition.

The *Nosal* rationale has yet to be tested in the Supreme Court, which could settle the issue, although it is gaining momentum both in other courts[198] and also regarding suggestions to amend the CFAA.[199] Although a *Nosal*-based interpretation of liability for

[197] See (n 173).

[198] For a list of cases following the Nosal rationale see Stephanie Greene and Christine N. O'Brien, 'Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct under the Computer Fraud and Abuse Act' (2013) 50 American Business Law Journal 1, 22-3.

[199] Rep. Zoe Lofgren (D-CA) and Sen. Ron Wyden (D-OR) have suggested the elimination of the term of exceeding authorised access and the retaining only of the term 'access without authorisation' which will mean as introduced in the Bill suggested by Ms Lofgren: '(A) to obtain information on a protected computer; (B) that the accesser lacks authorization to obtain; and
(C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information;' see Bill to amend title 18, United States Code, to provide for clarification as to the meaning of access without authorization, and for other purposes. (2013) 113 Congress, 1st Session,

virtual sit-ins would be consistent with claims of hacktivists arguing that their protest is not actually unauthorised,[200] it appears that, at least, for the prosecutions so far, the 'intended use' test in *Czubinski/Explorica* has been followed. However, discussions of the CFAA and a new bill are underway, potentially moving towards the *Nosal* approach.[201] Nevertheless, this discussion at least demonstrates how complicated and vague the legal framework can be, especially when applied to acts that were particularly designed to challenge the definitions of the cybercrime regime, such as those employed by hacktivists.

Compared to be above complications, the concept of authorisation is, for the moment at least, more clear-cut in the UK. The dominant rationale expressed in *R v Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America*[202] is that, when the use of authorisation to access certain information is not carried out for the purpose for which the authorisation was given, access exceeds authorisation. Consequently, in cases where a virtual sit-in targets a publicly accessible website with many users automatically reloading the page, their authorisation, although initially existing, exceeds its limits from the moment the protests action employs this access in order to disrupt the communication, which is not why the authorisation was initially provided. In another case, *DPP v Lennon,*[203] regarding the automatic bombarding of an email account with thousands of emails, the court argued that the purpose of the email account was to facilitate communication via email and authorisation was given to other users in order to send emails for that purpose rather than to send thousands of emails that would render communication actually impossible.[204] The court decided that such acts constituted modification of the email account that exceeded authorisation.[205] Therefore, DOS attacks, based on a similar rationale regarding authorisation, which is essentially similar to the *Czubinski/Explorica* rationale discussed at the beginning of this section, are likely to be considered unauthorised acts. Virtual sit-ins with the purpose of impairing rather than

<http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20-%20lofgren%20-%20061913.pdf> accessed 30 July 2013.

[200] DJNZ and The Action Tool Development Group of the Electrohippies Collective (n 62); Ricardo Dominguez, 'Electronic Disobedience Post-9/11' (2008) 22 Third Text 661.

[201] Zoe Lofgren and Ron Wyden 'Introducing Aaron's Law, a Desperately needed Reform of the Computer Fraud and Abuse Act' (*Wired,* 20 June 2013) http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/ accessed 21 June 2013.

[202] [1999] All ER (D) 972 (*Allison).*

[203] *DPP v.Lennon* [2006] All ER (D) 147 (*Lennon*).

[204] ibid.

[205] ibid.

getting actual information from a website are also likely to be considered unauthorised acts in the UK.

Naturally, with activities that actually entail an intrusion, such as defacements or data thefts, the lack of authorisation will be obvious and even more straightforward than virtual sit-ins, since usually there will not be any prior authorisation. Consequently in the UK, since the purpose is a crucial criterion for assessing the exceeding of authorisation, the case would be clear for hacktivist acts. However, if *Nosal* is followed in the US, there will be a disparity in a crucial element of the cybercrime provisions, namely authorisation, between the two jurisdictions, which could lead to difficulties in extraditing offenders from the US to the UK and could even lead the UK courts and legislature to reconsider their approach too.

3.3.4 Hacktivism and the link with cyberterrorism

Another major concern that relates to the computer damage offences and hacktivism is the inclusion of these offences in cyberterrorism legislation which further reinforce the link between hacktivism and cyberterrorism. In the US, for example, the USAPA has included the intentional damage offence, section 1030(a)(5)(A) in the definition of 'federal crime of terrorism'. The federal crime of terrorism is an offence that aims to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct.[206] An additional requirement for including section 1030(a)(5)(A) as a terrorist crime is the satisfying of the felony liability triggers (I) and (V) discussed above.[207] Hacktions can be linked to these felony liability triggers, as has been seen,[208] and, thus, could easily fit the description. Furthermore, hacktivist tactics also satisfy another element of the definition of 'federal terrorist crime', which is the goal of influencing government conduct.[209] The requirement for the act to be coercive or retaliatory is also an element that could relate to hacktivist actions against an unjust decision or policy. After all, as has been seen in the discussion of non-violence,[210] differentiating between coercive and non-

[206] According to 18 U.S.C. Part I Chapter 113B, Section 2332b (Acts of terrorism transcending national boundaries) Section (g)(5) federal crime of terrorism means 'an offence that aims to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct.'.

[207] See Part 3.3.1 The focus on damage and loss and the expansion of the scope.

[208] ibid.

[209] See (n 206).

[210] Ch 2, Part 3.2 Non-violence.

coercive protests is a very challenging process. For example, the often coercive and retaliatory hue of many of Anonymous' declarations, further blur attempts to distinguish hacktivism from cyberterrorism according to the definition given above. Moreover, as the *Fullmer*[211] case shows, the illegality of organising and perpetrating electronic civil disobedience (e.g. virtual sit-ins) was a crucial element in finding the defendants guilty of conspiracy to violate the Animal Enterprise Terrorism Act,[212] consequently further linking ECD to potentially terrorist activities.[213]

Apart from severe increases in penalties for those accused of terrorist computer damage offences provided in the Sentencing Guidelines,[214] the implications of the link between counterterrorist laws and hacktivism are serious in terms of surveillance and investigation. As Podgor argues, the consequence of adding section 1030(a)(5)(A) to the offences for federal terrorism is that it would essentially justify the authorities to intercept wire, oral and electronic communications and even allows the Secret Service to engage in investigations that relate to CFAA offences that might be linked to hacktivism.[215]

Similarly, the UK counter-terrorist provisions also link computer damage offences to cyberterrorism. The Terrorism Act 2000[216] gives a definition of terrorism, listing actions or threats to act, which, 'when designed to influence the government (including its agents and the police) or to intimidate the public or a section of the public, for advancing political, religious or ideological causes', could constitute a terrorist act. As the Electrohippies highlight, the term 'or', which was not initially part of the Bill, means that actions seeking to

[211] *Fullmer* (n 163).
[212] 18 U.S.C. Part I, Chapter 3, Sections 43(a)-(c). The penalties provided by this Act can be very high depending on the damage and losses they cause. For example, if the economic damage to the animal enterprise exceeds the amount of $10,000, the penalty could be a term of imprisonment of up to five years. (b)(2). The definition of economic damage (d)(3)(A) here includes loss as well.
[213] The protesters' behaviour also included other illegal elements, such as harassment and threats against employees of animal testing facilities, in addition to ECD tactics.
[214] According to the U.S.S.G. (n 142) Section 3.A.1.4, 'If the offense is a felony that involved, or was intended to promote, a federal crime of terrorism, increase by 12 levels; but if the resulting offense level is less than level 32, increase to level 32.' This would actually amount to 121-151 months of incarceration and a fine of up to $175,000.
[215] Ellen Podgor 'Computer Crimes and the Patriot Act' 17 Criminal Justice, 61, 62; The USAPA also includes extended provisions, concerning surveillance and interception powers with Internet Service Provider cooperation, securing electronic communications wiretaps and intensifying jurisdiction and enforceability of federal agencies and secret services. Dana L. Bazelon, Yun J. Choi, and Jason F. Conaty, 'Computer Crimes' (2006) 43 American Criminal Law Review 259, 269, 301-2; Tara M. Raghavan, 'In Fear of Cyberterrorism: An Analysis of the Congressional Response' (2003) Journal of Law Technology & Policy 297, 304-5.
[216] UK Terrorism Act 2000 (c .11).

influence the government could be considered terrorist acts without also requiring an intimidating effect on the public sentiment, which means the definition actually encompasses efforts to influence policy change – a basic goal for most protesters and hacktivist groups.[217]

The inclusion of electronic forms of protest is further established by section 1(2)(e) of the Terrorist Act 2000, which refers to threats or actions designed to seriously interfere with or seriously disrupt an electronic system, including acts outside the UK.[218] According to the explanatory notes to the UK Terrorist Act 2000, this law is designed to cover actions, which can have a devastating impact on modern networked society despite not being violent, yet, as far as explaining section 1(2)(e), they only add that it is meant to cover the serious disruption of key computer systems.[219] It has been argued that the term 'seriously' is adequate to differentiate between terrorism and effects, which can just be a 'costly nuisance', although others have deemed the definition wide enough to encompass traditional hacking and system impairment.[220] The Act also refers to activities outside the UK or against governments abroad,[221] thus potentially criminalising hacktivists that protest against governmental or financial websites of other countries.[222] Similarly to the US, the legislation allows the authorities to adopt very relaxed procedural standards, since, for example, a constable can arrest without a warrant someone whom he reasonably suspects to be a terrorist.[223] Naturally, if ECD acts are considered terrorist, those who incite such protests, such as hacktivist organisers and groups, could also be prosecuted for several inchoate offences, such as public provocation or recruitment.[224]

[217] The Electrohippies Collective (n 46).
[218] (1)(4)(a).
[219] Fafinski, 'Computer Misuse: The Implications of the Police and Justice Act 2006' (n 169) 55-56.
[220] Clive Walker, 'Cyber-Terrorism: Legal Principle and Law in the United Kingdom' (2005) 110 Penn State Law Review 625*,* 632; Out-Law.com, 'UK Law Makes Hacking an Act of Terrorism' (*Out-Law,* 21 February 2001) <http://www.out-law.com/default.aspx?page=1409> accessed 20 May 2011; Walden (n 57) 183; The Electrohippies Collective (n 46).
[221] Terrorism Act 2000, Section 1(4).
[222] See account of global hacktivist protests against Mexican President Website and Frankfurt Stock Exchange website. Dorothy E. Denning, 'Hacktivism: An Emerging Threat to Diplomacy' (2000) 77 Foreign Service Journal 43.
[223] See UK Terrorism Act 2000, Section 41(1). See more examples in Walker (n 220).
[224] Schjølberg (n 108); Logan also argues that the Terrorist Act 2006 is in fact so extensive, as to threaten those that express a controversial political opinion with deportation from the UK. Christina C. Logan, 'Liberty or Safety: Implications of the USA Patriot Act and the UK's Anti-Terror Laws on Freedom of Expression and Free Exercise of Religion' (2006) 37 Seton Hall Law Review 863*,* 865.

The concerns from analogising hacktivism to terrorism have induced attempts to differentiate hacktivist practices from terrorism. It has been suggested, for example, that for politically motivated hacking operations to be considered as cyberterrorism, they should cause so grave harm or damage as to generate fear comparable to that of destructive, offline terrorism.[225] Denning testified before the Special Oversight Panel on Terrorism Committee on Armed Services in the US House of Representatives in 2000 that 'EDT and the Electrohippies view their operations as acts of civil disobedience, analogous to street protests and physical sit-ins, not as acts of violence or terrorism. This is an important distinction. Most activists, whether participating in the Million Mom March or a Web sit-in, are not terrorists.'[226] Walker also argues that an important category of cyberterrorism is hostile activity on computer systems.[227] These hostile acts will most likely be defacements of websites, viruses and denial-of-service attacks that do not cause any physical damage, but can fundamentally compromise the provision of information and services.[228] However, only acts that could have the capacity to terrorise should require a special counter-terrorist law response.[229] For Walker, defacements or DoS attacks, even if violating cybercrime laws and their potential disruption to governmental computer systems is substantial, are unlikely to have the same impact on the lives of individuals as terrorism would in order to support the analogy of hacktivism to terrorism.[230] On a practical basis, important state and corporate infrastructures are now very difficult to infiltrate and manipulate due to increased security measures that makes attacks on such services far harder and requiring much more skill than that of average hacktivists.[231]

Even if terrorism-related prosecutions do not ensue, the legal link that exists between hacktivism and cyberterrorism could lead to further marginalisation of these protesters and the generation of more intense public censure, even for hacktivists acting in accordance to moral criteria, such as those discussed in chapter two. A characteristic example is the

[225] Clay Wilson, 'Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress', (Library of Congress, Congressional Research Service, Washington D.C. 2008) 4; Harinda Vidanage, 'Rivalry in Cyberspace and Virtual Contours of a New Conflict Zone: The Sri Lankan Case' in Athina Karatzogianni (ed), *Cyberconflicts and Global Politics* (Routledge, Oxon 2009) 146-161, 159.

[226] Cited in Dominguez (n 200) 663.

[227] Walker (n 220) 642.

[228] ibid.

[229] ibid.

[230] ibid, 643.

[231] Wall (n 43) 57.

withdrawal of the Electrohippies from the active hacktivist scene. [232] Risks of counter-terrorist sanctions could, however, also lead to a proliferation and radicalisation of protests, since excessive monitoring and punishment can lead to resentful reactions from determined hacktivists, who would abandon any self-regulation limitations.[233] Some of Anonymous' activities express such a tendency of 'cumulative extremism',[234] where apprehensions of online protesters induce more protests and lead to suggestions for more radical, covert attacks and even the design of anonymising tools for sit-ins.[235] In response, the authorities become even stricter towards hacktivists, propagating a circle of radicalisation that eventually also impacts on user experience with stricter regulations and overall surveillance being imposed from the authorities and more risk-rich network disruptions from reacting hacktivists. The reduction of self-regulated, ethical hacktivists in addition to the increase of more harmful and less principled ones would thus be exacerbated from the employment of cybercrime laws in ways that connect hacktivists to cyberterrorism.

The provisions mentioned above for the US and the UK are only indicative examples, since there are multiple regulations expanding counter-terrorist measures[236] that eventually imbue authorities with extra monitoring and enforcement powers against

[232] The Electrohippies Collective (n 46).

[233] Samuel (n 61) 54-55; Ayres and Braithwaite (n 2) 25.

[234] Roger Eatwell, 'Community Cohesion and Cumulative Extremism in Contemporary Britain' (2006) 77 The Political Quarterly 204.

[235] Anonymous 'AnonNews - Everything Anonymous' (*AnonNews,* 08 March 2011) <http://anonnews.org/?p=comments&c=ext&i=996> accessed 21 June 2013; Jon Leyden, 'Anonymous Unsheathes New, Potent Attack Weapon' (*The Register,* 04 August 2011) <http://www.theregister.co.uk/2011/08/04/anon_develops_loic_ddos_alternative/> accessed 11 September 2011.

[236] Apart from USAPA there are also other relevant acts such as the Homeland Security Act of 2002 116 Stat. 2135 and the Intelligence Reform and Terrorism Prevention Act of 2004, 118 Stat. 3638, 2004 (IRTPA).The US Criminal Code also includes an abundance of provisions that relate to terrorism, which are out with the scope of the current analysis; Also in the UK, beyond the Terrorism Act of 2000, which is the most relevant for our case, there is an abundance of inter-related and amending counter-terrorism Acts in the UK as well, such as the Anti-Terrorism, Crime and Security Act of 2001, (c.24), Prevention of Terrorism Act 2005, (c.2) the Terrorism Act 2006, (c.11), which all constitute a concerted effort to intensify the government's and law enforcement's capacity to monitor and punish activities, which might be even remotely and inchoately related to terrorism. For more detail see: Clive Walker, 'Clamping Down on Terrorism in the United Kingdom' (2006) 4 Journal of International Criminal Justice 1137; Logan (n 224)The arbitrariness has been somehow ameliorated with the changes introduced by The Terrorism Act 2000 (Remedial) Order 2011, No.631, which requires reasonable suspicion for the stop and search powers of the authorities.

undesirable political/ideological groups and their supporters, hacktivists included.[237] Although a detailed review of the very complex counter-terrorist legislation is beyond the scope of this dissertation, the analysis of some basic provisions is meant to establish the potential for the legal link between hacktivism and cyberterrorism and the prospective consequences of this link for hacktivists and users in general. Although counterterrorist prosecutions of hacktivists have not happened yet, as the court in *Nosal* argued, even if the state guarantees it will exercise discretion in prosecuting appropriate cases only, we should not rely on the discretion of prosecutors, as there is a risk that politically charged cases might tempt prosecutors to make use of their discretion in undue ways.[238]

3.4 Resources, information and lack of harmonisation

There are also some inherent general reasons why cybercrime legislation is an inappropriate tool for dealing with hacktivism. The inherent problems of extra-jurisdictional enforceability and lack of harmonisation and cooperation,[239] in conjunction with global, decentralised nature of hacktivism and its relation to different moral and political views, make the application of national law problematic, not only in terms of efficiency,[240] but also in achieving a relative degree of legal certainty. For example, the capacity of citizens to protest against issues they might feel strongly about, but might relate to other nations, in combination with the difficulties of apprehending and extraditing offenders from other states, leads to a very interesting disparity that the Internet's international reach exacerbates: Protesters from the UK or the US protesting against targets that are somehow linked to the US or the UK, are often prosecuted, as documented above.[241] Conversely, protesters are rarely prosecuted in cases where the protests could be against another state's websites, even if originating from countries, such as the US and UK, which have established liability for attacks originating from their territory against targets abroad.[242] In fact, in many cases, international efforts, such as virtual sit-ins against Iranian or Egyptian

[237] Logan (n 224) 869-71; Fafinski, 'Computer Misuse: The Implications of the Police and Justice Act 2006' (n 169) 56.

[238] *Nosal* (n 186) 3869-70.

[239] Gregor Allan, 'Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative' (2005) New Zealand Law Review 149, 150.

[240] See Part 1. Regulating hacktivism: The focus on 'command and control'.

[241] See Part 3.3.3 Unauthorised access and intentional damage.

[242] For jurisdictional reach of CFAA see Part 3.2 The applicable unauthorised access offences.

governmental websites would not even be investigated, if not encouraged, even when they were pre-announced with online videos by the same collective, Anonymous,[243] members of which are being investigated and persecuted in the US and the UK for similar activities against western corporate and governmental targets. Consequently, hacktivists feeling they are doing something acceptable, when protesting injustice abroad, might be faced with very harsh penalties, when they try to realise similar protests against websites of their own governments for their local injustices, even though cybercrime laws would consider all similarly disruptive activities equally criminal and prosecutable by the same authorities.

The above problem of disparate legal treatment of hacktivism internationally is further exacerbated by a lack of global harmonisation of approaches and penalties for cybercrime. Despite general harmonisation efforts,[244] as seen above, even on the issue of unauthorised access for example,[245] serious deviations have ensued between UK and US approaches. Even in the same jurisdiction, there are many different agencies that are burdened with dealing with cybercrime and, therefore, even national approaches might vary significantly, further impacting on international cooperation.[246] The penalties for cybercriminality between jurisdictions still vary widely, for example, even between countries of the advanced West, such as Sweden or Germany, which have adopted less punitive responses compared to the US-UK pole.[247] Despite the *Lufthansa* case, which exonerated virtual sit-ins

[243] Ellinor Mills 'Anonymous to Target Iran with DoS Attack' (*CNet,* 29 April 2011) <http://news.cnet.com/8301-27080_3-20058700-245.html> accessed 21 June 2013; Mojit Kumar 'Anonymous Hit Egyptian Government Websites as #Opegypt' (*The Hacker News*, 09 December 2012) <http://thehackernews.com/2012/12/anonymous-hit-egyptian-government.html> accessed 21 June 2013.

[244] Examples of harmonisation efforts are the promulgation and ratification of the Cybercrime Convention (n 148) by many states or the Framework Decision (n 146) on attacks against information systems, criminalising denial-of-service attacks and distribution of hacking software, as well as the discussions for a new cybercrime/cyberwarfare convention and a new EU Cybercrime Directive. OUT-LAW, 'Commission Proposes New EU Cybercrime Law' (*The Register,* 11 October 2010) <http://www.theregister.co.uk/2010/10/11/eu_new_cybercrime_law/print.html> accessed 10 November 2012; Daniel Shane, 'Think Tank Calls for 'Geneva Convention' on Cyber War' (*Information Age,* 04 February 2011)<http://www.information-age.com/technology/security/1599193/think-tank-calls-for-'geneva-convention'-on-cyber-war> accessed 10 November 2012.

[245] Part 3.3.3 Unauthorised access and intentional damage.

[246] As it is reported for example, in the US, at the congressional level, there are at least four committees with their relevant subcommittees that have jurisdiction over cybercrime decisions and different approaches and interests, consequently leading to a fragmentation of oversight and lack of uniformity in approaching issues of online criminality. See Benjamin S. Buckland, Fred Schreier, and Theodor H. Winkler,'Democratic Governance Challenges of Cyber Security' (*Geneva Security Forum,* 2012) <http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf> accessed 15 May 2013, 19.

[247] Despite the explicit criminalisation of denial of service attacks, other countries like Germany have retained lower maximum penalties. Nate Anderson, 'Germany Adopts "Anti-Hacker" Law; Critics Say

as expressive and non-coercive,[248] the fact that the protesters were not tried under computer damage laws makes the usefulness of that precedent questionable,[249] even in Germany, especially since DoS attacks have been explicitly criminalised recently.[250] Conversely, in more current US litigation, virtual sit-ins and their organising have been perceived as proof of coercive, criminal intentions, thus, resulting in very serious criminal charges for the organisers,[251] while guilty pleas and court decisions have resulted in heavy penalties for virtual sit-in participants both in the US and the UK.[252]

International harmonisation is further hindered by the decision of various states to operate as non-cooperative safe havens for cybercriminals.[253] Former Soviet Republics, for example, often operate as cybercrime havens due to organised cybercriminals influencing policy-makers through threats and bribes, thus, preventing the passing of relevant law or because propagating the problem of cybercrime results in financial assistance for dealing

It Breeds Insecurity' (*Ars Technica*, 28 May 2008) <http://arstechnica.com/security/news/2007/05/germany-adopts-anti-hacker-law-critics-say-it-breeds-insecurity.ars> accessed 20 May 2011; See Section 303a-b StGB (German Criminal Code) for data tampering and computer sabotage. Furthermore, in Germany these offences are prosecutable only after victim request, except for cases of serious public interest. See Section 303c StGB. The 10-year maximum is only explicitly provided for extremely serious acts of major economic loss, organised crime and hindrance of supply of vital goods and services or national security. See Section 303b4 StGB. In Sweden penalties are even lower, with even attacks on infrastructural services being punishable with no more than four years. See**:** European Network and Information Security Agency (ENISA) *Sweden: Country Report* (ENISA*,* 2011) <http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Sweden.pdf> accessed 15 February 2013.

[248] European Digital Rights, 'Frankfurt Appellate Court Says Online Demonstration Is Not Coercion' (*European Digital Rights,* 07 June 2006) <http://www.edri.org/edrigram/number4.11/demonstration> accessed 20 May 2011; Even before the exonerating appeal, the penalty for organising a virtual sit-in was a small fine. Thus, German citizens could consider these activities legitimate in their country and participate only to find that they are charged under new EU legislation or even be extradited to the US.

[249] The virtual sit-in was tried under charges of coercion (Noetigung) Section 240 StGB, which provides it is an offence to use force or (certain other means) in order to coerce someone to act against their will. See Peter E. Quint, 'Civil Disobedience and the German Courts: The Pershing Missile Protests in Comparative Perspective' (Taylor and Francis e-Library, 2007)

[250] Sylvia M. Kierkegaard, 'Here Comes the 'Cybernators'!' (2006) 22 Computer Law & Security Report 381, 387; Federico Biancuzzi, 'Achtung! New German Laws on Cybercrime' (*Security Focus*, 10 July 2007) <http://www.securityfocus.com/columnists/448> accessed 20 May 2011.

[251] *Fullmer* (n 163).

[252] See (n 189); In the UK, hacktivist Weatherhead received an 18 month prison sentence after pleading not guilty regarding charges of conspiracy to impair a computer regarding the Anonymous protests against Paypal. See Ch 3, (n 41).

[253] The Convention on Cybercrime (n 148) and the Framework Decision(n 146) are indicative of the aim to achieve more harmonisation and cooperation, with little binding power and still much to be done to reach satisfactory cooperation levels. See Walden (n 57) 328-9; Schjølberg (n 108) 17.

with the problem from richer, industrialised nations.[254] Lewis further submits that countries that desire the expression of dissent against countries, such as the US, for example, would perhaps refrain from criminalising or prosecuting cyberdeviants that might be expressing a form of dissent that haven-countries would regard to be in accordance with their political interests.[255]

The problem of harmonisation and jurisdictional reach has been a consistent problem identified by the early theorists of cyberlaw, such as Johnson and Post and Goldmsith.[256] Although Goldsmith had countered their concerns by highlighting the applicability of processes like extradition,[257] the political nature of hacktivism, along with its global character might render extraditions, and therefore, the whole cybercriminal structure, inefficacious. This would be particularly so, considering that, even between states that have very similar approaches to cybercrime, such as the US and UK, there has been a reluctance to extradite cyberdeviants.[258] As Aas highlights, the globalising interdependence of information systems has not yet managed to impose a full homogenisation of penal approaches, with cultural specificities influencing the perception of criminality and the nature and extents of punishment.[259] Harmonised approaches, thus, become increasingly difficult when the activities to which varying legal regimes must be applied entail elements that are morally and ideologically contested, and, thus, subject to different treatment between different regimes.[260] For example, a discord is to be expected since the salience of the problems of cybercrime can be much higher in industrialised nations than in less advanced societies.[261] The issue of hacktivism might be of no importance in Middle East

[254] Brian C. Lewis, 'Prevention of Computer Crime Amidst International Anarchy' (2004) 41 American Criminal Law Review 1353.
[255] Ibid.
[256] Part 1. Regulating hacktivism: The focus on 'command and control'.
[257] ibid.
[258] BBC, 'Gary McKinnon Extradition to US Blocked by Theresa May' *(BBC,* 16 October 2012) <http://www.bbc.co.uk/news/uk-19957138> accessed 10 November 2012; As is submitted in the APIG Report for the CMA, there has never been an extradition of offenders to the UK. All Party Internet Group (APIG) 'Revision of the Computer Misuse Act': Report on an inquiry by the All Party Internet Group (2004) <http://www.cullen-international.com/cullen/multi/national/uk/laws/cmareport.pdf> accessed 14 August 2013, 15.
[259] Aas (n 55) 173-5.
[260] Gregor Urbas, 'Criminalising Computer Misconduct: Some Legal and Philosophical Concerns' (2006) 14 Asia Pacific Law Review 95, 107; Podgor (n 215) 736; Different perceptions of free speech and legal protesting could influence how these acts are perceived, while different criminal approaches with less punitive frameworks could allow for more protests.
[261] Lewis (n 254).

countries, but there could be many protesters joining hacktions against US governmental systems from these jurisdictions.

3.5 Conclusion

This section has reviewed the deficiencies of the cybercriminal law regimes in dealing with hacktivism, highlighting mainly their lacking in clarity, consistency, efficiency and proportionality. The application of a criminal law regime that is a priori flawed and not designed to deal with the delicate moral and practical distinctions between crime, hacktivism and cyberterrorism, with these deficiencies being also applicable on a global scale due to jurisdictional expansion of cybercrime regimes, eventually intimidates moral protesters or radicalises them, essentially generating more numerous and severe online disruptions and endangering the rights and liberties of many users. However, since the Internet is still largely technically managed by private corporations, a question that arises is whether the role of private companies with their command of technological solutions and network management capacities could function as a balancing force to the excesses and deficiencies that have been documented so far in this chapter. The following part will discuss the impact of private online intermediaries, service and content providers, on hacktivism and will discuss the potential regulatory deficiencies.

4. The role of private actors

4.1 Private regulators, privacy and hacktivism

As discussed above,[262] the importance of private actors in regulating online behaviours has been documented even from the early debates between cyberlaw theorists, as a more efficient way of regulating the Internet, compared to traditional state-based solutions. Private actors have gradually attained a prominent role in regulating cyberspace, either

[262] See Ch 1, Part 1.1 Defining regulation and also 1. Regulating hacktivism: The focus on ‘command and control’.

directly through a combination of private terms of use and code-based tools,[263] or indirectly, through lobbying governments for policies[264] or as proxies for enforcing governmental decisions, since governments delegate duties to online companies in relation to network security and policing.[265] In relation to hacktivism, the current focus on law-based regulation has eventually resulted in subordinating private actors, mainly those creating and managing Internet networks and software, into serving the dominant 'command and control' approach. The creation of software that facilitates control has been a result, not only of direct, but mostly indirect, ordering through the promulgation of regulations by the state which influence other regulating forces, such as code writers and corporate actors, and induce changes in software and hardware functions and Internet structures.[266] States, thus, employ incentivising or coercive mechanisms to steer code-making towards facilitating information-control.[267] The opaque and automated nature of code-based solutions that do not need to go through a public legitimisation process that state laws and regulations have to acquire,[268] can further exacerbate the danger of states imposing unreviewable restrictions through private actors employing opaque technological controls.[269]

Private actors' actions can, thus, impact on hacktivism, both in terms of organising and expression, but also in terms of further facilitating criminal sanctions through monitoring and policing. As McNamee suggests, for example, although some measures might be taken in order to prevent the potential for excessive or arbitrary policing by private actors, the

[263] See examples of America Online (AOL) or Google in Dawn C. Nunziato, 'The Death of the Public Forum in Cyberspace' (2005) 20 Berkeley Technology Law Journal 1115; More to be discussed below in this section.

[264] A typical example is the cases of big studios in relation to copyright protections, where lobbying for new, stricter and more expansive laws has been persistent. See the example of the Sonny Bono Copyright Extension Term Act. Krystal E. Noga, 'Securitizing Copyrights: An Answer to the Sonny Bono Copyright Term Extension Act' (2007) 9 Tulane Journal of Technology & Intellectual Property 1*,* 9-10.

[265] The example of the Chinese Government, which has passed numerous policies obliging ISPs and even internet cafes to participate in policing cyberspace is characteristic of how the state can employ private actors for indirect regulation. See Vasileios Karagiannopoulos, 'China and the Internet: Expanding on Lessig's Regulation Nightmares' (2012) 9 SCRIPTed 150.

[266] Lessig, *Code v.2.0* (n 2) 62-7, 72, 80.

[267] ibid 133.

[268] Christoph B. Graber, 'Internet Creativity, Communicative Freedom and a Constitutional Rights Theory Response to "Code Is Law" (Lucerne: i-call, The Research Centre for International Communications and Art Law, University of Lucerne, Working paper 03, 2010) 6.

[269] Jody Freeman, 'Real Democracy Problem in Administrative Law' in David Dyzenhaus (ed), *Recrafting the Rule of Law* (Hart Publishing, Oxford 1999) 335.

political pressures, the increasing legislated obligations for such companies, the lack of strict procedural safeguards and the fact that the preservation of rights is not a task for private actors result in invasions of free speech and privacy.[270] Furthermore, the merging of access providers and media companies exacerbates the problems of bias and selective prioritisation of online traffic according to the business' conglomerates interests.[271] The role of many Internet companies in regulating hacktivist activity online and more specifically during the provision of their services to hacktivist groups can be even more pertinent, since online conglomerates are often targeted, or, at least, criticised by hacktivists and would, therefore, have an increased interest in restricting expression that can be critical towards these companies and their policies.[272]

Current legislation has had an impact on internet intermediaries, transforming them into police enforcers by enabling or forcing the unaccountable and extensive information exchange between the authorities and the online content and service providers. For example, the US government passed a law that granted legal immunity many US telecommunications companies, thus protecting them from lawsuits that had arisen from the role of these companies in warrantless surveillance of online activities of users; [273] an initiative which, inevitably, raises serious accountability concerns. The current US National Security Agency Prism project exposed by an NSA contractor, Snowden, is indicative of the extent of the collaboration of the government with private telecommunications companies in policing citizen communications in generalised and opaque ways.[274] The European Court

[270] Joe McNamee, 'The Slide from "Self-Regulation" to Corporate Censorship' (*European Digital Rights*, Brussels 2011) <http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf> accessed 15 February 2013, 8-11.

[271] ibid 12.

[272] See the creation of the Back Orifice software. Ch 1, Part 2.2.1 The first era of hacktivism and the birth of electronic civil disobedience; Anonymous have also targeted multiple software and hardware corporations for their support towards the Cyber Intelligence Sharing and Protection Act that promotes online security and increased surveillance procedures. The list includes companies such as Intel, Verizon, Facebook, US Telecom and IBM. Gianluca Mezzofiore 'Anonymous Targets Facebook, IBM, Intel and AT&T in Operation Defense Phase II' (IBTimes, 13 April 2012) <http://www.ibtimes.co.uk/articles/327682/20120413/cispa-operation-defense-anonymous-pledges-attack-intel.htm> accessed 21 June 2013.

[273] Elana Schor 'Telecoms Granted Immunity in US Wiretapping Probe' (*The Guardian*, 20 June 2008) <http://www.guardian.co.uk/world/2008/jun/20/georgebush.usa accessed 21 June 2013.

[274] Stephen Braun et al. 'Secret to Prism Program: Even Bigger Data Seizure' (*Associated Press*, 15 June 2013) <http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure> accessed 21 June 2013; Kim Dotcom 'Prism: Concerns over Government Tyranny Are Legitimate' (*The Guardian*, 13 June 2013) <http://www.guardian.co.uk/commentisfree/2013/jun/13/prism-utah-data-center-surveillance> accessed 21 June 2013.

of Human Rights in *KU v Finland*[275] has also accepted that legislation legitimises ISPs data retention and facilitation of surveillance, especially for reasons relating to crime prevention.[276]

Even when companies want to prioritise user privacy, opposing the authorities might be hard to achieve. Twitter, for example, had initially declined to disclose data of its users, but recently it has been forced to comply with a decision by a San Francisco court requesting the private details of bloggers, even if the illegal act was realised from citizens abroad using the service.[277] Challenging the decision would require the users to also access the San Francisco courts, thus making review of these decisions very costly and inaccessible to plain users.[278] Additionally, as Levy reports, Google or Comcast, for example, customarily avoid asking any questions or provide notice to customers when they are served subpoenas to disclose customer information regarding a criminal investigation and instead focus only on whether the form has been filled out correctly and has been issued by courts of competent jurisdiction.[279] He acknowledges, though, that ISPs, as opposed to Google, would not have access to the speech they transmit and, hence, they could not check on the potential reasonableness of the subpoena claim.[280] Consequently, online activists cannot rely on private actors to protect the privacy of protesters against governmental requests and question the authorities, since most companies will want to avoid coming into conflict with state agencies. Large online conglomerates have been accused of collaborating even with the most oppressive of regimes, when profit was involved. The case of Yahoo, Microsoft,

[275] (2008) ECtHR 2872/02.

[276] Buckland, Schreier and Winkler (n 246) 22; Additionally, anti-piracy legislation, such as the Digital Economy Act 2010 in the UK, currently demonstrates the intention to engage ISPs into actively deterring, if not monitoring, users for copyright infringement and potentially even imposing penalties in the form of blacklisting or imposing connectivity restrictions, even leading major ISPs to challenge, unsuccessfully the imposition of such obligations upon them. See case comment in Sam De Silva and Faye Weedon, 'A Future Less Certain for the Digital Economy Act?' (2011) 17 Computer and Telecommunications Law Review 149.

[277] See Nigel Green and Josh Halliday, 'Twitter Unmasks Anonymous British User in Landmark Legal Battle' (*The Guardian,* 29 May 2011) <http://www.guardian.co.uk/technology/2011/may/29/twitter-anonymous-user-legal-battle> accessed 02 September 2012; The same was done in a New York case for an Occupy Wall street protester account. Cyrus Farivar, 'NY Judge Compels Twitter to Reveal User's Data' (*Ars Technica,* 02 July 2012) <http://arstechnica.com/tech-policy/2012/07/ny-judge-compels-twitter-to-reveal-user-data/> accessed 02 September 2012.

[278] See Green and Halliday (n 277).

[279] Paul A. Levy 'Responding to Prosecutors Seeking to Identify Anonymous Bloggers — Google and Other ISP's Could Learn from the Mainstream Media' (*Consumer Law and Policy Blog,* 17 November 2010) <http://pubcit.typepad.com/clpblog/2010/11/responding-to-prosecutors-seeking-to-identify-anonymous-bloggers-google-and-other-isps-could-learn-f.html> accessed 23 November 2012.

[280] ibid.

Google, or Cisco collaborating with the Chinese regime that expects from the companies operating in China to filter politically controversial communications, police content and even allow the authorities' access to private users is the most characteristic example.[281]

4.2 Private regulators and hacktivist speech

Furthermore, legislation relating to the management of content in online communications encourages ISPs to censor controversial speech and activities based on notices for the takedown of alleged illegal content. For example, the Communications Decency Act[282] and the Digital Millenium Copyright Act[283] in the US and the E-commerce Directive in the EU,[284] which has been transposed into UK law by the Electronic Commerce (EC Directive) Regulations of 2002,[285] all include 'safe harbour' provisions that encourage companies hosting online content to expeditiously take down postings, groups or even websites that they have been notified are illegal, often without examining the validity of the claim.[286]

As Frydman and Rorive argue:

> [U]nder the current legal provisions, ISPs are strongly encouraged to quickly remove any material when notified, even informally, by any third party that these data are infringing, defamatory, dangerous, seditious, inaccurate or otherwise illegal or damaging. This situation generates an obvious "chilling effect" on freedom of speech

[281] Amnesty International,'Undermining Freedom of Expression in China: The Role of Yahoo!, Microsoft and Google' (*Amnesty International*, 2006) <http://web.amnesty.org/library/pdf/POL300262006ENGLISH/$File/POL3002606.pdf> accessed 20 May 2012.

[282] 47 U.S.C. Section 230(c).

[283] 17 U.S.C. Section 512.

[284] Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-commerce Directive)[2000] OJ L 178, art. 14.

[285] No.2013, art.19.

[286] Frank Pasquale, 'Trusting (and Verifying) Online Intermediaries' Policing' in Berin Szoka and Adam Marcus (eds), *The Next Digital Decade: Essays on the Future of the Internet* (Techfreedom, Washington D.C. 2010) 360.
See analysis in Organisation for Economic Co-Operation and Development, *The Economic and Social Role of Internet Intermediaries* (*OECD*, 2010)< http://www.oecd.org/internet/ieconomy/44949023.pdf> accessed 23 February 2013, 10-1.

> on the Internet, which is not consistent with the protection guaranteed by Article 10 of the European Convention on human rights.[287]

McNamee also adds that:

> Companies such as Facebook come under intense pressure in relation to individual incidents that attract the interest of politicians and/or the press. These create strong pressure for private companies to regulate their clients in order to prevent possibly illegal activities (and this will be exacerbated by any weakening of the intermediary liability regimes), it also creates pressure to regulate any activity that creates a liability or public relations risk for the company. Intermediaries design their terms and conditions in order to prepare for exactly such an eventuality.[288]

Furthermore, intermediaries usually manage their services based on contract terms and conditions that are non-negotiable. These terms of use establish certain standards of allowable speech, which are mainly enforced with the help of software that automatically assesses the existence of those standards and through responding to user notifications. The usual vagueness and broadness of the terms of allowable speech enables content-managing companies to discretionarily limit content and user-interaction to what they would consider acceptable. Moreover, as Nunziato submits, Google and other companies, based on their sponsored advertisements regulated by their terms of service, have consistently declined to host advertisements of controversial political advocacy groups with a politically or religiously critical content.[289] Due to the dominant market position of prominent content- and service-providing companies, such as Google, private policies can result in the censoring of a great amount of protectable political or social criticism, which will not be accessible on prime search engine spaces or popular websites.[290] Activist groups' views that could often entail much controversy, would, thus, be under more danger of facing filtering and blocking, either as a result of code-based, opaque enforcement of terms of use or of more conservative users' flagging. For example, both Twitter and Facebook have censored Anonymous' accounts regarding various operations or blocked the hashtag

[287] Benoit Frydman and Isabelle Rorive, 'Regulating Internet Content through Intermediaries in Europe and the USA' (2002) 23 Zeitschrift für Rechtssoziologie 41*,* 56.
[288] McNamee (n 270) 34.
[289] Nunziato (n 263) 1123-4.
[290] ibid.

of Anonymous.[291] Legislation is, essentially, structured in such a way that encourages and justifies as safe corporate practice wholesale infringements on speech and privacy in order for online corporations to avoid the potential of liability. Simultaneously, these above safe harbour provisions and the policies they encourage fail to promote the potential for more understanding and enrichment of perceptions that the engagement of additional actors could bring and also lead to the disregarding of the increasingly important role of online corporations for user privacy and speech in the fully privatised cyberspace.

On the same note, online money-processing services, such as Paypal or Visa, have similarly demonstrated a tendency to succumb to political pressures and decline to offer their services to politically controversial websites, such as Wikileaks, despite there being no official investigations or criminal charges against the latter's activities.[292] In fact, Wikileaks won the case against Visa last year for its decision to stop processing donations.[293] Such restrictive tactics violate the rights of subscribers and censor politically controversial actors that attract political attention with their actions. Such policies, as the case of Wikileaks demonstrate further exacerbate the problem, leading to further protests and radicalisation of the victimised users and their supporters.[294] Eventually, the acts of these money processing companies impact, not only on the rights of the protesters and the websites, but also compromise, through the proliferation of reactionary protests to their policies, themselves, their customers and the general public due to the increase in protests that their unjustified and politically motivated policies can cause. A typical example of this is the Anonymous' protests against Paypal and Visa after their refusal to serve Wikileaks and the impairing impact this had on these organisations' websites in addition to preventing users from accessing their services of short periods is indicative of how unjustified policies of corporations that perform important functions for the viability of private online organisation can lead to reduction of overall security online.

[291] Sn Vikas, 'Anonymous' Operation India Removed from Facebook and Twitter' (*The Next Web,* 12 June 2011) <http://thenextweb.com/in/2011/06/12/anonymous-operation-india-removed-from-facebook-and-twitter/> accessed 30 August 2012.

[292] Muhammad Ali, 'Anonymous, the Wikileaks Defenders clarify: We are not Hackers, we won't steal your Credit Cards' (*Geekword*, 2010) <http://www.geekword.net/anonymous-pr/> accessed 16 January 2011; Deanna Zandt, 'Are the Cyber Battles with the Enemies of Wikileaks the New Civil Disobedience?' (*Alternet,* 13 December 2010) <http://www.alternet.org/story/149183/are_the_cyber_battles_with_the_enemies_of_wikileaks_the_new_civil_disobedience> accessed 28 September 2011.

[293] Ch 2, Part 3.5 Last resort.

[294] Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism.

It is, therefore, obvious that engaging private corporate actors in regulation in ways that subordinate them primarily to governmental and legislative desires and also allow them to decide on the types of free speech that will be prioritised or even be available on their networks can have indirect negative implications for hacktivism. The harms mainly relate to the organisation of the hacktivist groups and their actions, reducing the opportunities for critical and politically controversial expression in ways that can often be arbitrary and excessively restrictive of users' rights. As McNamee argues, although private actors on the Internet were initially given self-regulatory powers, the concept of self-regulation has now taken the form of 'devolved enforcement, surveillance and extra-judicial punishment of allegedly illegal activities.'[295] Inevitably, the subordination of private actors to the dictates of an expanding criminalisation of online activities, not only restricts their positive regulatory potential, but compromises the interests of controversial political groups, both in terms of expressing their views and respecting their privacy.

Before drawing our final conclusions regarding the criticisms of the current approach towards hacktivism, the last, but very crucial stage will be to analyse the enforcing actors of the legislation, namely the prosecutors and the judiciary.

5. Hacktivism, prosecutors and the courts[296]

5.1 The role of prosecutors

5.1.1 Prosecutorial power and the new mentality

As mentioned in the previous chapters, a crucial aspect of regulating hacktivism is the existence of discretion in punishment, and the capacity and willingness for contextual assessments and the potential for justly deserved punishment. Prosecutors are dominant actors in criminal justice processes, as they have the power to decide whether to press

[295] McNamee (n 270) 7.

[296] Hacktivism is realised from a distance and, thus, the police, although a crucial part of enforcement in offline crime, have a very secondary role here in terms of exercising discretion and apprehending offenders red-handed. Therefore, their role is mainly to facilitate the orders of prosecutors and will not be analysed separately, since prosecutors are the dominant executive agents.

criminal charges and the nature of those charges, and to terminate prosecutions.[297] For example, the US Attorneys' Manual provides that prosecutors are responsible for initiating and declining prosecution; selecting charges; entering into plea agreements; opposing offers to plead nolo contendere; entering into non-prosecution agreements in return for cooperation; and participating in sentencing.[298]

Although prosecutors cannot and should not act as substitutes of the legislature and the courts, they usually retain interpretive freedom and influence on sentencing as well.[299] Prosecutors are often perceived and expected to act, not only as law-enforcers, but as more creative agents with multiple roles, from interpreters of law and state policy facilitators to expressors of community sentiment.[300] These multiple functions are reflected in the number of elements prosecutors must assess when deciding on prosecutions. For example, the US Attorneys' Manual[301]suggests that prosecutors should take into account the priorities of federal law enforcement, the deterrent effect the prosecution will have on the offender, the nature and seriousness of the crime and the history of the accused, his personal blameworthiness, his willingness to collaborate with the authorities for resolving other crimes and the consequences of convicting that person.[302] If the prosecutor decides that the person was morally culpable only for a minor participation in a criminal conspiracy and that the motive behind such an act was morally worthy, he/she could decide that prosecution would not be the best solution.[303]

Prosecutors' generally wide discretion is normally unreviewable since they are considered the most knowledgeable of the case details, deterrence value, the state's enforcement goals and the link of the case to an overall enforcement plan.[304] In the UK, for

[297] Amie N. Ely, 'Prosecutorial Discretion as an Ethical Necessity: The Ashcroft Memorandum's Curtailment of the Prosecutor's Duty to Seek Justice' (2004-5) 90 Cornell Law Review 237, 242-3; Kent Greenawalt, *Conflcts of Law and Morality* (Oxford University Press, New York 1989) 350-1.

[298] United States Department of Justice 'United States Attorney's Manual' (1997) <http://www.justice.gov/usao/eousa/foia_reading_room/usam/ accessed 21 June 2013, Chapter 9-27.110 A; For UK see Crown Prosecution Service, 'The Code for Crown Prosecutors' (2010) <http://www.cps.gov.uk/publications/code_for_crown_prosecutors/> accessed 15 February 2013.

[299] Ely (n 297) 244-6.

[300] Greenawalt (n 297) 352; Crown Prosecution Service (n 298) 3.

[301] US Department of Justice (298) Chapter 9-27.110.

[302] Ely (n 297) 244.

[303] US Department of Justice (298) Chapter 9-27.230 Section B.4.

[304] It is argued that courts seldom review the prosecutors' decisions based on allegations of improper charges and usually only when there is a constitutional challenge behind the allegation, such as racial discrimination. There is also a lack of review of prosecutorial decisions in relation to overcharging

example, prosecutors decide on the adequacy of evidence for ensuring conviction and also establish that there is a serious public interest in pursuing the case and punishing the offender, while retaining the final say, even after a review process.[305] Prosecutors in the US can prosecute based on the existence of probable cause - an even more relaxed criterion than the UK realistic prospect of conviction.[306] However, even for the stricter UK prosecutorial standard of requiring a realistic chance to convict, the expansion of criminal law both in terms of criminalising behaviours and extending culpability renders most prosecutions much more viable. In both jurisdictions, the prosecutors' views are considered acts of the executive that courts cannot review on the basis of the principle of the separation of power.[307] Only recently, UK courts have demonstrated a tendency to more actively review prosecutorial decisions, mainly to assess whether prosecutors might have disregarded prosecutorial guidelines and policies.[308]

Prosecutorial discretion also creates serious concerns for the balance of power between the various actors of the criminal justice process. The power of prosecutors has been further extended due to the promulgation of a wide and overlapping array of criminal offences that give prosecutors the tools to pursue prosecutions as they see fit.[309] Consequently, the current expanding and punitive form of legislation in addition to the wide, unreviewable discretion has transformed the traditional role of prosecutors, giving them a dominant role at the expense of judges, juries, parole authorities and defence lawyers and ultimately, offenders to exercise important rights.[310] The war on crime has also increased tolerance of power abuses by the authorities, presumably realised for the sake of

defendants to obtain plea agreements, pre-textual charges and failures to disclose exculpatory material to juries. Podgor (n 215) 734, 736; In the UK, courts could suggest to the Crown Prosecution Service to reconsider a decision to prosecute or not, but the decision ultimately lies with the CPS. Crown Prosecution Service, 'Appeals: Judicial Review of Prosecutorial Decisions' (21 May 2009) <http://www.cps.gov.uk/legal/a_to_c/appeals_judicial_review_of_prosecution_decisions/> accessed 24 November 2012; The courts in England have reflected the tendency to impose a very light review to prosecutorial discretion, accepting reviews mostly for cases of abusive use of discretion. Yoav Dotan, 'Should Prosecutorial Discretion Enjoy Special Treatment in Judicial Review?: A Comparative Analysis of the Law in England and Israel' (1997) 3 Public Law 513, 513-5.

[305] Crown Prosecution Service (n 298).

[306] Nick Vamos, 'Please Don't Call It "Plea Bargaining"' (2009) Criminal Law Review 617, 620.

[307] Dotan (n 304)515; Rebecca Krauss, 'The Theory of Prosecutorial Discretion in Federal Law: Origins and Developments' (2009) 6 Seton Hall Circuit Review 1.

[308] Dotan (n 304) 518-9.

[309] Glenn Reynolds, 'Ham Sandwich Nation: Due Process When Everything Is a Crime' (Legal Studies Research Paper 206, University of Tenessee, Tenessee 2013) <http://ssrn.com/abstract=2203713> accessed 20 June 2013.

[310] Simon (n 25) 35, 38-9.

public safety.[311] Particularly in cases that attract public attention, which could, for example, include hacktivists targeting major companies or governmental websites, prosecutors may be reluctant to demonstrate leniency for fear of appearing irresponsible or inconsiderate of the public's safety.[312]

This tendency is further reinforced by the generally accepted, yet - as research has proven - inaccurate, presumption that the public would want harsher penalties for offenders than those handed down.[313] The need of prosecutors to appease the public can lead them to avoid decisive punishment reductions or non-prosecutions, since such lenient actions would alienate many parties interested in risk-control, from politicians and security firms to the media or the public.[314] Moreover, the bypassing of restrictions to prosecutorial discretion, such as being unbiased and abiding by due process standards, is further intensified by the legal training of prosecutors, which is adversarial in common law jurisdictions and oriented towards achieving convictions, rather than attempting to uncover the truth.[315] The prosecutorial harshness against Swartz, which eventually led to his suicide under the pressure of having to face charges amounting to potentially up to 50 years in prison for illegally downloading and publishing thousands of copyright-protected academic articles from proprietary databases, has been considered an indicative case of such a polarisation between prosecutors and online activists.[316]

Prosecutors also favour increasingly punitive solutions because the prospect of very high penalties induces alleged offenders to accept the lower penalties that prosecutors offer for guilty pleas.[317] As Reynolds argues, prosecutors often employ many felony charges against alleged offenders, a practice which, essentially, increases the risk of even one felony being

[311] Even though federal prosecutors are more distanced than regular state prosecutors, being elected in countrywide elections, they still have to make similar considerations. ibid 42-3, 72-3.

[312] Kenneth J. Melilli, 'Prosecutorial Discretion in an Adversary System' (1992) Brigham Youth University Law Review 669, 688; Paul Rosenzweig, 'Overcriminalization: An Agenda for Change' (2004) 54 American University Law Review 809, 811.

[313] See discussion in Ch 3, 2.2.3 Are highly punitive sanctions for ECD utilitarian?.

[314] Anonymous, for example, have argued about there being a political bias in decisions to prosecute hacktivists, which can be perceived by the lack of interest by prosecutors in finding the perpetrators of denial- of-service attacks against the Wikileaks website, which is also a serious network compromise. Anonymous, 'Anonymous Press Release: Open Letter from Anonymous to the UK Government' (*Anonops*, 27 January 2011) <http://anonops.webs.com/ANONYMOUS-PRESS-RELEASE_27-01-2011.pdf> accessed 10 November 2012.

[315] Melilli (n 312) 686, 694.

[316] See Ch 3, Part 2.2.3 Are highly punitive sanctions for ECD utilitarian?; Reynolds (n 309) 1.

[317] Beale, 'The News Media's Influence on Criminal Justice Policy' (n 66) 422-3.

accepted by the court, thus naturally inducing offenders to concede to plea bargains.[318] In fact, the widely unreviewable discretion combined with the proliferation of plea bargaining, which is employed to resolve almost 90% of cases in the US,[319] and facilitated by multiple overlapping laws, allows for prosecutors to be, not only the initial assessors, but also the ultimate adjudicators, since most of the cases never reach the courtroom.[320] Alschuler, in his criticism of plea bargaining, argues that a substantial part of the actual penalty imposed relies on a tactical decision that is independent to any of the proper aims of criminal proceedings or the alleged offenders actions or personal characteristics.[321] Considering that prosecutors become also adjudicators of facts and culpability through the process of offering guilty plea bargains to alleged offenders, the process of fact finding and contextual assessment of motivations is significantly shorter and, inevitably, not as meticulous.[322]

Arbitrary powers of prosecution have led to unequal treatment of suspects and to factually innocent citizens succumbing to prosecutorial pressures to plead guilty.[323] As Davis argues, prosecutors that feel they might not be able to achieve a conviction in court will have strong incentives to induce suspects to accept plea bargains, which would guarantee them an otherwise doubtful conviction,[324] especially since in the US prosecutors can prosecute even if acquittal seems likely.[325] In the UK, arbitrary abuses of plea bargaining are more restricted due to the many safeguards that prevent prosecutorial excesses, such as the need for a realistic prospect of conviction and the prohibiting prosecutors from using many additional charges in order to induce pleas.[326] However, it has been argued that, both in the US and the UK, plea bargaining has been used as a tool for increasing the

[318] Reynolds (n 309) 3-4.

[319] Russell L. Christopher, 'The Prosecutor's Dilemma: Bargains and Punishments' (2003) 72 Fordham Law Review 93.

[320] Krauss (n 307) 7-9.

[321] Albert Alschuler, 'Implementing the Criminal Defendant's Right to Trial: Alternatives to the Plea Bargaining System' (1983) 50 University of Chicago Law Review 931, 932.

[322] Krauss (n 307) 8-9.

[323] See examples in Samuel R. Gross et al., *Exonerations in the United States 1989-2003* (University of Michigan, 2004) http://www.mindfully.org/Reform/2004/Prison-Exonerations-Gross19apr04.htm; Angela J. Davis, *Arbitrary Justice: The Power of the American Prosecutor* (Oxford University Press, Oxford 2007) 48-52.

[324] Davis (n 323) 44.

[325] Vamos (n 306) 621.

[326] ibid 622-3.

prosecutions of minor offenders, while more serious, resource-intensive and hard to convict cases are bypassed, what has been called 'defining deviance down'.[327]

Consequently, even though plea bargain penalties might appear milder than what sentences could be incurred in court, the fact that prosecutors often have the upper hand to convince suspects to plead guilty and the fact that many of them could be innocent or at least guilty of less serious offences than those they are charged for,[328] would result in higher punishments than those deserved. Again the US system is far more extreme, allowing the potential range of sentencing for multiple offences to be more extensive and reliant on prosecutorial desires than the more moderate UK system.[329] This trend is further exacerbated by the discouragingly expensive and slow nature of court proceedings which often appears daunting and can easily exhaust activists, financially and psychologically, and induce them to choose the faster and, on its face, less arduous and risky process of guilty pleas.[330] Consequently, the cybercrime regime, with its broad interpretations, overlapping provisions and its high maximum penalties is an ideal tool for prosecutors in achieving pleas, but also in portraying punitive guilty plea offers as lenient, compared to what the actual penalty could have been.

On their behalf, hacktivists, being often young,[331] would wish to avoid the complications and higher sentences of an actual trial, thus, agreeing to plead guilty. Most prosecutions of hacktivists have been resolved by guilty pleas, with only Weatherhead in the UK pleading not guilty - a decision that resulted in a penalty of 18 months imprisonment.[332] By offering similar guilty plea deals to a protester charged with intentional and reckless damage (Guzner) and to a protester charged only with negligent damage (Mettenbrink), prosecutors have also demonstrated a tendency not to differentiate between varying degrees of culpability of hacktivists and to disregard the retributive principle of treating equal cases

[327] Garland (n 24) 117-9.

[328] ibid.

[329] Vamos (n 306) 623.

[330] Fawzia Cassim, 'Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study' (2009) 12 Potchefstroom Electronic Law Journal 35, 45.

[331] For example, the four members of Anonymous prosecuted for the Paypal attacks in the UK were between 16-25 years old, when the offence was perpetrated. Brid-Aine Parnell 'Brit Mastermind of Anonymous Paypal Attack Gets 18 Months' Porridge' (*The Register*, 24 January 2013) <http://www.theregister.co.uk/2013/01/24/uk_anonymous_hackers_sentencing_payback/> accessed 26 January 2013.

[332] See ibid; see also (n 252).

equally.[333] Even if the case does not result in an actual conviction for hacktivists, the filing of felonious charges can have a very serious impact on those facing these charges both practically and psychologically.[334]

Consequently, considering the adjudicatory power of prosecutors and the side-lining of context and personal characteristics for more tactical decisions that can have publicisable results which would demonstrate efficiency, one can argue that the criminal justice system operating with a focus on achieving convictions for populist reasons, rather than attributing justice based on the moral qualities of the suspects, is a problematic tool for dealing with hacktivism. With hacktivists relying excessively on discretionary assessments of moral culpability, it is inevitable that excessive reliance on prosecutorial rather than judicial decision-making would reduce the attention given to the moral details of their cases, with the prosecutorial decisions and the suggested penalties reflecting this bypassing of potential mitigating factors and producing undeserved penalties.

5.1.2 The practical concerns of prosecutors

The above trends are reinforced by some practical considerations. The limited resources for prosecuting online law-breakers induce prosecutors to focus on easy-to-resolve cases. Consequently, targeting hacktivists that are generally easier to identify and prosecute compared to more seasoned cybercriminals and publicising these achieved prosecutions, provides easier and publicly-appeasing results for prosecutors.[335] As it has been argued, despite the fact that hacktivists mostly desire to shame their targets, rather than inflict actual damage, 'law enforcement officials are certainly going to want to make an example of anyone they can bring in'.[336] Nevertheless, it has to be conceded that the radicalisation

[333] (n 252).

[334] Some of the consequences can be pre-trial incarceration, loss of employment, social stigmatisation, criminal defence costs, as well as emotional stress: Melilli (n 312) 672; Protesters have talked about the impact their prosecution has had with many being unable to find work until the case is resolved and one even threatening to commit suicide if he is convicted: Smith and Reilly (n 88).

[335] Peter Swire, 'No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime' (2009) 7 Journal on Telecommunications & High Technology Law 107*,* 108.

[336] Jaikumar Vijayan ''Anonymous' Arrests Tied to Paypal DDoS Attacks, FBI Says' (*Computer World,* 20 July 2011) http://www.computerworld.com.au/article/394256/_anonymous_arrests_tied_paypal_ddos_attacks_fbi_says/ accessed 10 November 2012.

of hacktivists has mutually contributed to hacktivism becoming a focal point for the authorities.

The difficulty in assessing culpability for cyberdeviants is also related to the obscurity in assessing motivations and intentions behind cyberactivities done at a distance.[337] The difficulty of assessment of context leads decision-making to rely on strictly-set guidelines and further weakens the possibility of relying on contextual assessments and moral distinctions between malign cybercriminal offenders and moral cyberprotesters. The difficulty to decide is also intensified by the inability of criminal justice professionals to distinguish between positive and negative cyberdeviant incidents, as this difficulty significantly influences prosecutorial decisions by obscuring potential moral and practical distinctions.[338] Prosecutors are often educated to view any hacking-related activity as generally anti-social.[339] Therefore, in addition to a potentially adversarial rationale dictating prosecutorial decision-making, established perceptions regarding cybercriminals would often reduce the chances for more understanding and tolerant prosecutorial decisions. In sum, the various criminal justice trends, professional mentalities and practical concerns of prosecutors suggest that unbiased procedures based equally on efficiency and proportionality concerns and consequently, tolerant attitudes are likely to be restricted.

The last stage in this regulatory structure is the assessment of the courts' attitudes towards hacktivism and their general tendencies. Do judges and juries offer any hope for balancing the punitive, calculating exaggerations facilitated by social norms, legislative decisions and prosecutorial, largely unchecked, power?

[337] Trevor Thompson, 'Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the White Hats under the CFAA' (2008) 36 Florida State University Law Review 537, 567.

[338] Skibell (n 58) 941; Wall (n 43) 163-4, 7.

[339] DJNZ and The Action Tool Development Group of the Electrohippies Collective (n 62) 270; Civil disobedience had been compared with plain street criminality in the US ever since the 60s and 70s, when crime was emerging as a core policy interest. See: Beale, 'What's Law Got to Do with It?' (n 52) 40-1; UK and US officials have expressed their perspective of members of the Anonymous as socially detached hackers that have unavoidable criminal and anti-social tendencies, characterising them even as terrorists. Vijayan (n 336).

5.2 The role of courts in regulating hacktivism

5.2.1 The general power of the judiciary and the role of sentencing guidelines

The role of courts in ultimately enforcing or balancing the various normative and legislative policies discussed in this chapter renders them a fundamental stage in the current regulatory structure that is predominantly driven by the cybercriminal justice system. Courts normally shape sentencing decisions according to moral considerations as well as the offence's impact on society and decide on whether and how severely to punish.[340] Although the courts had in previous decades been a strong faction of governance, combining elements of legislative and executive power with personal expertise and neutrality, their social policy-making power has gradually been weakened.[341] There has been a rift between the executive-legislature and the courts, with prosecutors gradually shifting responsibility for lenient punishments of offenders to the liberal tendencies of courts and aligning with the legislature in weakening the judiciary's role.[342] Discretion has currently shifted to the executive, and yet, prosecutors lack the judicial culture of neutrality and the experience in independent punishment assessment, with prosecutorial decisions being more tactical and mostly unreviewable.[343] The weakening of courts, which are those most specialised in assessing contextual and moral elements within the criminal justice process, inevitably leads to disregarding motives and socio-political conditions and the capacity of judges to suggest mitigation or exoneration; a trend that, of course, has implications for deciding on activities such as hacktivism.

The above tendency to detract discretionary power from courts is also exacerbated by the subordination of judicial decision-making to sentencing guidelines that, in turn, have been amended, so as to increasingly limit judicial discretion, attacking sentencing disparity and abolishing parole.[344] The strict sentencing guidelines have been considered a crucial

[340] Carl Cohen, 'Civil Disobedience and the Law' (1966) 21 Rutgers Law Review 1, 16-7.

[341] Simon (n 25) 111-2.

[342] However, judges have often been blamed as overtly lenient. Zlotnick (n 60) 247-9; Hough and Roberts (n 313).

[343] Zlotnick (n 60) 212-4.

[344] ibid 232-8; Michael A. Wolff, 'Evidence-Based Judicial Discretion: Promoting Public Safety through State Sentencing Reform' (2008) 83 New York University Law Review 1389*,* 1398-1400; Julian V.

sentencing tool in both US and UK, even after they were made non-mandatory in the US.[345] US courts must also consider the guidelines, even if not mandatory, and are allowed to depart from them, if the sentencing council has not considered certain mitigating or aggravating factors.[346]

Nevertheless, departure rates are higher in the UK than the US as the criminal history is calculated differently and could cause departures (not factored in the guidelines like the US). In most cases, however, departures are upward, as UK guidelines focus more on aggravating, rather than mitigating circumstances.[347] Moreover, despite the contextual criteria introduced by the sentencing guidelines, in the US, these guidelines contain many more aggravating than mitigating circumstances, eventually allowing for multiple increases in punishment ranges through similar criteria.[348] For example, in a recent case considering the extraction of email accounts data from the network of AT&T, the perpetrator's sentence range was increased both for use of sophisticated means and use of a special skill, which were considered overlapping factors.[349]

A guidelines-based calculation of sentences thus creates generalised criteria for assessing punishment severity.[350] Reliance on general guidelines for sentencing is, of course, a wider issue with the current structure of criminal justice, but also becomes very detrimental for hacktivists. This is because the existence of predefined, generalised

Roberts, 'Sentencing Guidelines and Judicial Discretion' (2011) 51 British Journal of Criminology 1, 5-6.

[345] See *US v Booker,* 543 U.S. 220 (2005)(*Booker*) rendering the guidelines advisory after 2005, but still considered basic for sentencing: U.S.S.G. (n 142) 2, 12. However, as the U.S.S.G. (n 142) explains, departures are allowed only when the court finds 'an aggravating or mitigating circumstance of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines that should result in a sentence different from that described.' 18 U.S.C. Section 3553(b); Reliance on sentencing guidelines with binding effect is now common in the UK (after the Coroners and Justice Act of 2009) and even New Zealand. ibid 5-6, 13-4; However, especially in the UK, there is a qualification in the duty of the courts to follow the guidelines based on whether, such a decision would be contrary to the interests of justice. Coroners and Justice Act 2009 Section 125(1)(b).

[346] Alexa Chu Clinton, 'Taming the Hydra: Prosecutorial Discretion under the Acceptance of Responsibility Provision of the Us Sentencing Guidelines' (2012) 79 The University of Chicago Law Review 1467*,* 1471-2.

[347] See Roberts (n 344) 7-8.

[348] See United States Sentencing Commission, '2011 Federal Sentencing Guidelines Manual ' Chapter 2B1.1.

[349] *US v Auernheimer*, Criminal No.: 2:11-cr-470 (SDW) (Dist. Court, New Jersey 2013) Defendant's Sentencing Memorandum <http://www.scribd.com/doc/130262013/u-s-v-auernheimer-def-sentencing-memo> accessed 21 June 2013.

[350] Simon (n 25) 129.

mitigating and mainly aggravating circumstances creates a more mechanistic way of assessing punishment ranges and, therefore, would often generate problems for assessing deviant acts, the moral elements of which might not be translatable into fixed sentencing criteria. Essentially, some of the positive aspects of hacktivism, such as an increase in political sensitisation or the expressive enablement it entails on a global scale against the reduced speech opportunities online[351] cannot be easily categorised. It is, however, exactly these abstract elements that highlight the distinction of moral hacktivist actions from criminality and support the hacktivists' justifiability and any subsequent lenient responses.

Discretion in every step of the criminal justice process has been considered favourable to criminals and thus undesirable for the zero-risk policies that dominate contemporary criminal justice reforms.[352] However, the consistent war on discretion and a gradual 'conservatisation' of the judiciary has led it to refrain from frequent deviations, entrusting the correctness of prosecution and penalty to the executive.[353] In general, , in a system dominated by prosecutorial discretion, plea bargains and sentencing guidelines, the courts seem to play a much lesser role than that which is ideal for cases with the contextual and moral complexity that hacktivist actions often entail. These restrictions in the actual adjudicatory role of the judge demonstrate yet another reason why the current criminal justice system is a problematic approach, if relied upon as a single, dominant method for regulating hacktivism.

5.2.2 The influence of judicial culture

In addition to the general guided framework within which judges must currently operate, trends in judicial decision-making and legal reasoning can strongly influence the judiciary.[354] As Holmes has argued: 'The felt necessities of the time, the prevalent moral and political theories, intuitions of public policy, avowed or unconscious, even the prejudices, which judges share with their fellow men, have a good deal more to do than the syllogism in

[351] Ch 2, Part 1. Free expression and hacktivism.

[352] Simon (n 25) 101.

[353] Zlotnick (n 60) 242, 254; Simon (n 25) 113, 128-30; Even after *Booker* (n 345), Congress has still managed to limit any downward deviations from the guidelines as much as possible. See ibid 166-8; Roberts (n 344) 7.

[354] Ian McLeod, *Legal Theory* (2nd edn Palgrave MacMillan, New York 2003) 137; Frank B. Cross, 'Decisionmaking in the US Circuit Courts of Appeals' (2003) 91 California Law Review 1475, 1464.

determining the rules by which men should be governed.'[355] Research has also demonstrated that dominant rationales are bound to influence decisions in a discriminatory way against those labelled as anti-social.[356] Therefore, the prominent normative and legal trends of security and risk-control will, according to what Holmes describes above, influence judges' perceptions of risk-generating behaviours, with hacktivism being one such category of risk-rich activities. As Garland clarifies, '[T]he social and economic determinants of "the outside world" certainly affect the conduct of penal agents (police officers, judges, prison officials, etc.), but they do so indirectly, through the gradual reshaping of the rules of thought and action within a field that has what sociologists call a "relative autonomy"'.[357] Moreover, judges are also influenced by their ideologies and the socio-political specificities, in which they live, work and develop.[358] Consequently, in addition to established social norms directly influencing judicial decision-making, the documented lack of trust of the public towards the judiciary and the calls for more punitive sentences could have an impact on judges' sentencing choices, especially for high profile cases.[359] Common stereotyping of hacktivism as criminal or terrorist,[360] subconsciously internalised and integrated in decisional patterns, is also likely to influence judicial responses and judges would inevitably have to employ additional effort to remain unbiased.[361]

A potential bias could also be connected with the ideological influences flowing from the usually high socio-economic background of judges,[362] which could potentially impede their understanding and acceptability of radical and innovative protesting of marginalised minorities, for which, however, ECD might often be a feasible dissent tactic. Moreover, the understanding of online activist tactics will also be hindered by the judges' level of familiarisation with new technologies, as their cognitive background is important for

[355] Oliver Wendel Holmes Jr., *The Common Law* (Paulo J. S. Pereira and Diego M. Beltran (eds), University of Toronto Law School Typographical Society, Toronto 2011) 5.

[356] See: Daniel L. Real and Honorable John F. Irwin, 'Unconscious Influences on Judicial Decision-Making: The Illusion of Objectivity' (2010) 43 McGeorge Law Review 1, 3-4, 6.

[357] Garland (n 24) 24.

[358] Donald Nicolson, 'Ideology and the South African Judicial Process-Lessons from the Past' (1992) 8 South Africa Journal on Human Rights 50; See analysis of various researches on the influence of ideology and the factors that influence ideology itself in Joel Grossman, 'Social Backgrounds and Judicial Decision-Making' (1966) 79 Harvard Law Review 1551, 1556-7.

[359] Hough and Roberts (n 313) 14-20. See also Ch 3, Part 2.2.3 Are highly punitive sanctions for ECD utilitarian?.

[360] Part 2. The normative framework and its impact on hacktivism.

[361] Real and Irwin (n 356) 6-7.

[362] Nicolson (n 358) 285; Grossman (n 358) 1553-4.

justifying their ultimate decision.[363] Judges are often not in tune with the latest technological advances, which is obvious in cybercriminal law interpretations and decisions that, in turn, inevitably impact on the decisions' justness and efficaciousness.[364] The shaping of judicial opinions on technical issues also becomes more reliant on security experts' and victims' assessments, which can often exaggerate the dangers and implications of the offence in question for their own interests.[365] Precedent also plays a big role in shaping decisions of the judiciary and it would appear that the few cases that have reached the courts so far, as well as the few guilty pleas prosecutors have induced, suggest a bleak future for ECD.[366]

5.2.3 The role of the jury

The jury is also a fundamental part of the criminal justice system, albeit far more so in the US than the UK. Juries operate as the voice of the community and since criminal trials are evaluations of culpability, jurors can decide on the suspect's blameworthiness.[367] Juridical assessments normally provide a limitation to overcriminalisation, governmental excesses and the enforcement of morally obsolete laws,[368] while also informing the legislature, the executive and the courts of current moral perceptions of certain behaviours.[369] Moreover, sentencing decisions can be influenced by the jury's power to acquit, even against law and

[363] Cross (n 354) 1477-8.

[364] Skibell (n 58) 926-7; Urbas (n 108) 104, 106; The current Twitter ban on alleged members of Anonymous in relation to the trial for the Paypal attack as a bail condition is also indicative of a lack of understanding, since the convergence of platforms and the multitude of platforms Anonymous are using are numerous, even excluding Twitter: The Smoking Gun 'Judge Lifts Twitter Ban on "Anonymous" 14' *(The Smoking Gun,* 19 March 2012) <http://www.thesmokinggun.com/documents/judge-lifts-anonymous-twitter-ban-145792> accessed 30 August 2012.

[365] Wall (n 43) 17-8, 23-4; Jennifer Granick 'Faking It: Calculating Loss in Computer Crime Sentencing' (2005) 2 I/S: A Journal of Law and Policy 207, 218.

[366] Matthew Lippman, 'Civil Disobedience: The Dictates of Conscience Versus the Rule of Law' (1986) 26 *Washburn Law Journal 233,* 251-2; Cross (n 354) 1464-6; See James L. Cavallaro, 'The Demise of the Political Necessity Defense: Indirect Civil Disobedience and United States v. Schoon' (1993) 81 California Law Review, 351 discussion on justification defences on whether CD-related precedent has to a very large extent been decided against the protesters.

[367] Michael Cahill, 'Punishment Decisions at Conviction: Recognizing the Jury as Fault-Finder' (2005) University of Chicago Legal Forum 91, 95.

[368] Richard Myers, 'Requiring a Jury Vote of Censure to Convict' (2009) 88 North Carolina Law Review 137*,* 152.

[369] ibid 142-3.

fact or, more moderately, to return a verdict for a lesser offence.[370] The power of the jury to acquit, despite condemning facts, has been named 'jury nullification', because juries ultimately nullify the law they have declined to enforce - a power relating to ancient precedent of juridical powers and due process rights.[371] In instances of nullification acquittals, jurors usually consider the law supporting the prosecution unjust or regard the specific case as outwith the scope and purpose of the law so that applying it would be against their conscience and beyond their role of assessing guilt and attributing justice.[372] Nullification or mitigation could also happen in cases where none of the above pertains, but the jury thinks the offender had overwhelming moral reasons for her actions.[373] As West argues, constitutional amendments and rules protecting jury verdicts allow the jury to acquit a defendant without explaining its decisions and without the decision being appealable due to the double jeopardy clause.[374] Therefore, the judiciary has the potential in theory to facilitate more procedurally consistent and substantively just processes and decisions, which would be important for hacktivists attempting to avoid sanction by promoting their moral characteristics.

Juries are also influenced by tendencies that dominate the contemporary socio-political realities and discourses and, subsequently, shape the citizens' cognitive experience and common symbolisms from which they can draw analogies.[375] Therefore, public beliefs about crime online and publicised, salient events can greatly influence jurors' perceptions with a great likelihood of a negative predisposition towards hacktivism. Any potential jury bias will also be harder to overcome than the one discussed in relation to judges, since the majority will be lacking the strong disciplined education for objectivity and reliance on legal

[370] Martin C. Loesch, 'Motive Testimony and a Civil Disobedience Justification' (1990) 5 Notre Dame Journal of Law, Ethics & Public Policy 1069*,* 1099-1100; Greenawalt (n 297) 360-1.

[371] Robert Hall, 'Legal Toleration of Civil Disobedience' (1971) 81 Ethics 128, 135, 137; Bernard D. Lambek, 'Necessity and International Law: Arguments for the Legality of Civil Disobedience' (1987) 5 Yale Law & Policy Review 472, 479.

[372] Greenawalt (n 297) 365-6. In the UK, the case of *R v Ponting* [1985] Crim. LR 318 is a characteristic example of jury nullification, where the jury accepted the argument of the defendant that Ponting's acts to reveal confidential information were in the public interest and acquitted him contrary to the directions of the court.

[373] Greenawalt (n 297) 365.

[374] Jessica L. West, 'Is Injustice Relevant? Narrative and Blameworthiness in Protester Trials' (Temple Law Review Forthcoming; Vermont Law School Research Paper No. 11-13, 2013) <http://ssrn.com/abstract=2247518> accessed 17 May 2013, 47.

[375] Dennis J. Devine et al., 'Jury Decision Making: 45 Years of Empirical Research on Deliberating Groups' (2000) 7 Psychology, Public Policy and Law 622, 636; Beale, 'The News Media's Influence on Criminal Justice Policy' (n 66) 402, 448-9.

principle that judges have.[376] As has been argued, prosecutors can exert a strong influence on jurors, which as Chief Judge Wachtler has said, could be convinced to even indict a ham sandwich.[377]

Even if juries could be sympathetic to the protesters causes, the fact that the courts have generally precluded the hearing of necessity defences on behalf of political protesters in the past further restricts the ability of hacktivists to present and explain their new cases with their specificities to a jury in more detail.[378] This defence presupposes that the judge will allow the jurors to consider factual evidence presented by the suspects on a potential choice of evils that led to the law-breaking at hand.[379] In the US, necessity has traditionally been accepted as a core justification incorporated in the Model Penal Code (MPC). The basic elements of the defence can be found in the US MPC, Section 3.02: '(1) Conduct that the actor believes to be necessary to avoid a harm or evil to himself or to another is justifiable, provided that: (a) the harm or evil sought to be avoided by such conduct is greater than that sought to be prevented by the law defining the offense charged; and (b) neither the Code nor other law defining the offense provides exceptions or defenses dealing with the specific situation involved; and (c) a legislative purpose to exclude the justification claimed does not otherwise plainly appear.'

Necessity has only recently been accepted in English law, initially as a defence of 'duress of circumstances'.[380] Under the premise of duress, UK courts have considered this defence as an excuse,[381] rather than justification, analogising it to regular duress.[382] Rendering

[376] Freda Adler, 'Socioeconomic Factors Influencing Jury Verdicts' (1973) 3 New York University Review of Law and Social Change 1, 1-2; Real and Irwin (n 356) 1-3, 7-8.

[377] Reynolds (n 309) 4-5; The phrase is attributed to US Chief Judge, Sol Wachtler, who advocated abandoning grand juries, as they were very prone to prosecutorial influences and let judges decide, so that prosecutorial excesses could be tempered. Marcia Kramer and Frank Lombardi, 'New Top State Judge: Abolish Grand Juries & Let Us Decide' (*New York Daily News,* New York 1985) 3.

[378] Cavallaro (n 366) 356-7.

[379] Daniel Farrell, 'Paying the Penalty: Justifiable Civil Disobedience and the Problem of Punishment' (1977) 6 Philosophy & Public Affairs 165, 176.

[380] Chris M.V. Clarkson, Heather M. Keating and Sally R. Cunningham, *Criminal Law: Text and Materials* (7th edn Thomson Reuters Ltd, London 2010) 353.

[381] Excuses do not render the act justified due to external circumstances but relate to the perpetrator and whether he she had full capacity to understand the implications of her actions, so that she can be considered morally reprehensible and thus punishable for them. Matthew R. Lippman, *Contemporary Criminal Law: Concepts, Cases, and Controversies* (Sage Publications, London 2010) 217-8.

[382] Clarkson, Keating and Cunningham (n 380*)* 277; Courts declined to accept the applicability of such an excuse in CD cases, finding that the will of the defendants was not overwhelmed by the threatened harms. ibid, 356; See *R v Howe* [1987] 1 AC 417; *R v Jones (Margaret)* [2005] QB 259.

necessity an excuse poses the burden of demonstrating that the threatened harm inevitably mentally coerced the offender to act in a certain way, something which, especially in cases of indirect CD is absolutely inapplicable as the protesters' actions are voluntary and not the result of coercion. Due to the long history that the US has demonstrated in relation to necessity compared to the UK, the analysis here will mostly focus on the US.

Necessity fulfils a corrective function for actions which entail a typical violation of a legal proscription, yet considerations of conventional public morality are eventually considered more important than the good protected by the specific offence overwhelm the prohibition included in the specific offence.[383] The Ninth Circuit has articulated a four-pronged evidentiary test that defendants have to satisfy for the jury to hear their defence. The elements are: (a) that the defendant chose the lesser harm of the two; (b) the law-breaking was meant to prevent an imminent harm; (c) he/she reasonably anticipated a causal relation between the law-breaking and the harm avoided; and (d) there was no other legal alternative to breaking the law.[384] Indirect CD protesters have had difficulties establishing the reasonable belief that the protest could prevent the harm/social injustice in question[385] and also to satisfy the requirement of the exhaustion of legitimate alternatives[386]. In *US v Schoon*[387] the court explicitly declared that the defence would not be employable for indirect CD.

The acceptance of this defence for hacktivist acts has not been tested. It would appear, however, that the indirect nature of hacktions would also be covered by the *Schoon* approach arguing for non-applicability of the defence for indirect law-breaking. In any case, hacktivists would be increasingly challenged to satisfy the requirements, such as the reasonableness of their belief in the necessity of their protest for averting the protested harm and the lack of legal alternatives, especially since in many cases, hacktions are realised as precursors to other legitimate protests and means of amelioration by bringing attention to a social injustice. The prohibition of necessity further exacerbates the trend of

[383] Robert F. Schopp, *Justification Defenses and Just Convictions* (Cambridge University Press, Cambridge 1998) 168-9.

[384] *US v. Dorrell,* 758 F.2d 427, 430-31 (9th Cir. 1985) cited in *US v Aguilar*, 883 F.2d 662, 693 (9th Cir. 1989)

[385] *US v Cassidy,* 616 F.2d 101 (4th Cir. 1979); *US v May,* 622 F.2d 1000 (9th Cir. 1980), *cert denied,* 449 U.S. 984 (1980).

[386] *US v Montgomery,* 772 F.2d 733 (11th Cir. 1985); *Dorrel* (n 384).

[387] 22 Ill.971 F.2d 193 (9th Cir. 1991)(*Schoon*); See analysis in Cavallaro (n 366).

courts in the US to routinely exclude protester motivation-related evidence as irrelevant,[388] consequently, intensifying the marginalisation of protester speech, even though reduced speech opportunities is a dominant reasons for illegal protest in the first place.[389]

Similar defences based on preventing state policies that violate higher laws have also been used, employing the argument of a potential violation of international law as evidence of a definite, serious harm that needs to be mitigated by the lesser evil of CD.[390] Citizens can employ such a defence to justify acts that aim to prevent harm from happening or negating a policy that is already in effect, realising serious crimes against humanity.[391] The defence provides that any person which has not been involved in the offensive action can intervene to prevent the commission or ongoing realisation of any crime if the measures he employs are not disproportionate to the particular context.[392] The only requirement is that there is a reasonable belief in the existence of an imminent or existing violation of a higher law and, even if the reasonable belief is mistaken, the defence may still be asserted.[393] Similarly to necessity, the reasonable belief in the existence of a harm to be averted could render behaviours excusable and should be interpreted as a mistake-based excuse that exculpates the defendant for the putatively justified conduct without rendering it lawful or even permissible.[394] Courts have often declined to accept this defence on the basis that the defendants lacked standing, since the fact that someone has been a citizen with an interest in making the government act within the bounds of the Constitution would not afford her standing to challenge the government's actions.[395] For example, the court in *US v May*[396], found that the harms alleged were too distant and general in relation to the protesters to justify their actions.

However, not all courts have declined to allow this defence. In *Mass. v Carter*, the judge and the jury acquitted the protesters after hearing that the justification of their illegal protests was based on efforts to prevent crimes of the Central Intelligence Agency (CIA) in

[388] West (n 374) 20, 26, 29.
[389] See Ch 2, Part 1. Free expression and hacktivism.
[390] Bernard D. Lambek (n 371) 484-7.
[391] John A. Cohan, 'Civil Disobedience and the Necessity Defense' (2007) 6 Pierce Law Review 111, 166-7.
[392] ibid 168.
[393] ibid.
[394] Schopp (n 383) 6-7.
[395] Cohan (n 391) 169.
[396] *US v May* (n 385).

South America.[397] Even in the UK, the higher law defence has been accepted by the jury in the form of lawful excuse, which renders lawful an act to prevent a more serious crime.[398] For example, in *R v Saibene and Others*, after being advised by the judge, the jurors acquitted the remaining protesters in relation to charges of conspiring to cause criminal damage to the premises of an armament company that was collaborating with Israelis against Palestine. The basis of the argument was that the company was assisting in the perpetration of war crimes, which were prohibited under international law that supersedes national law and that all legal alternatives had been exhausted.[399] However, the case has been severely criticised and the judge was even formally reprimanded for influencing the jury with personal anti-semitic remarks.[400]

The general rejection of defences for political cases, despite the few exceptions mentioned, has been based on another argument too: that acquittals would produce decisions, which would exceed the power of the jury as an assessor of facts,[401] thus, violating the political question doctrine. Opponents of the nullification potential of the jury that is facilitated through the employment of the necessity or higher law defences argue that juries go beyond assessing facts and end up assessing the justness of a law or political decision, thus allowing the courts to act for the legislature or the executive, which would violate the core democratic principle of the separation of powers.[402] The legal or political issues that courts might implicitly decide upon, if necessity and higher law defences are allowed, are, however, covered, by the 'pre-emption factor'.[403] This means that a policy is approved as legitimate on the presumption that its consequences have been deliberated by the executive or the legislature and have been formally accepted.[404]

The contemporary trend to predominantly not allow the necessity/higher law defences to be heard by the juries is especially important for political protesters cases, since research has aptly demonstrated that juries will often use their nullification powers if they are

[397] *Mass. v Carter* No. 8745-JC-0091A (Dist. Court., Hampshire County, Mass.1987).
[398] *R v Saibene and others* [2010] Lewes Crown Court.
[399] ibid.
[400] Joshua Rozenberg 'Buthurst Normal Reprimanded' (*Standpoint Magazine*, 07 October 2010) <http://standpointmag.co.uk/node/3462 > accessed 21 June 2013.
[401] West (n 374) 47-8.
[402] This doctrine forbids courts to decide on political matters and decisions, as being out with their adjudicative powers according to the democratic principle of separation of powers. Cohan (n 391) 122-3; Lippmann, 'Civil Disobedience' (n 366) 248-9.
[403] Cohan (n 391) 144.
[404] ibid.

allowed to hear the defences.[405] Consequently, the elimination of that prospect for the jury and the defendants totally deprives protesters of a potentially mitigating solution. As research has also shown, the public tends to be more lenient when allowed to hear the specifics of a criminal case and allowing the defence could provide an extensive account of the motives and the whole context of the protest.[406] In addition to general trends to consider motivation-related evidence as irrelevant,[407] this rejection, thus, becomes even more important, particularly since juries have demonstrated leniency, when familiarised with the facts of a political protest, despite its controversy.[408] In fact, as research has shown, jurors are prone to find a person less blameworthy, if she has a good motive or generally good character.[409] The denial of the opportunity to assess culpability more holistically often leads to a more mechanistic application of laws and again seems to disregard crucial differentiations between prima facie similar offences.[410] In the case of hacktivism, where the tactical distinctions are much less important than the moral culpability elements, bypassing contextual elements that influence the protesters' ultimate blameworthiness, such as evidence on motives and injustices protested, could result in sentencing that is inconsistent with public perceptions of the protesters' culpability and which is thus more likely to be disproportionate.[411]

6. Conclusion

This chapter has analysed the social norms and dominant symbols shaping cybercrime perceptions and laws, the legal provisions and their impact on hacktivism and the law and policy enforcement trends by state authorities, the judiciary, but also private actors online that have the power to influence the governance of Internet speech and socio-political organising. The main conclusion drawn in this chapter is that the current regulatory tools and methods employed in relation to hacktivism are very likely to produce illegitimate

[405] Devine et al. (n 375) 629-30.
[406] See Ch 3, Part 2.2.3 Are highly punitive sanctions for ECD utilitarian?.
[407] West (n 374).
[408] Cavallaro (n 366) 360-1.
[409] West (n 374) 40-1.
[410] ibid 40.
[411] ibid.

results, both in terms of efficiency and public well-being, but also in attributing deserved punishments and preserving a balance of justice.

More particularly, the policies adopted disregard civil liberties and user rights, with the problem becoming more intense for actors with the characteristics of hacktivists the actions of which entail higher risks and thus end up being condemnable in the contemporary security climate. Current regulations are focused on minimising damage, loss and controversial uses of information and networks and therefore, appear insensitive to moral culpability and benign motives, while also failing to provide satisfactory mechanisms of accountability and review processes for users. Furthermore, the employment of traditional, hierarchical notions of regulation through state law, fails to take into account the novel characteristics of online communities and the new perceptions and forms of activity online, attempting instead to subordinate any activity that challenges established presumptions to the dictates of an incumbent 'command and control' approach.

Secondly, the current regime also appears to be inefficacious or counterproductive in many aspects, as it predominantly employs criminal law to deal with online acts that by their nature are meant to challenge traditional notions of criminal law both morally and practically in terms of applicability and enforcement. Furthermore, where additional actors are employed, such as Internet intermediaries, these are also treated often as proxies for enforcing the cybercriminal laws for reducing risk and promoting strict security and information control. The analysis, however, has demonstrated that these laws and policies can also often fail to prevent serious cybercriminality for which they are mainly created due to issues of enforceability, focusing instead on less demanding cases of hacktivist protesters. At the same time, the vague and disproportionately punitive cybercrime regime leads to self-censorship of morally considerate hacktivists, while also radicalising other parts of the hacktivist community due to the legal regime's perceived illegitimacy. This inevitably results in fuelling less moral and more harmful practices of political disruption. Considering, therefore, the increasing attention that has been given to hacktivism and the important deficiencies identified in relation to the current methods and tools that are employed to regulate such phenomena, an effort to generate conditions that could facilitate a better, more efficient and just framework for dealing with hacktivism seems necessary. The next chapter will attempt to address the problems identified and provide suggestions on how these issues could be improved.

CHAPTER 5
REGULATION AND HACKTIVISM: WHAT CAN BE CHANGED?

The analysis so far has demonstrated that hacktivists' link to civil liberties and user norms, such as privacy and freedom of information and speech, as well as hacktivism's often global and legally ambiguous character, significantly challenge, morally and practically, attempts to regulate these acts through the criminal justice regime. More particularly, the current regulatory conditions are not structured or enforced in ways that would allow the evaluation of the special nature of hacktivism that potentially renders it politically legitimate and also enable the choice of more just and efficient sanctions. In many cases, hacktivism exacerbates existing flaws of the current regime, the society's moral panics, the excessive vagueness and punitiveness of the legal regime, the arbitrariness of its enforcers, the lack of harmonised approaches and the failure of conflicting national cybercrime laws to deal with hacktivism timely and efficiently. The current approach was shown to often produce unjust results through overtly harsh penalties and unaccountable policing and sentencing processes. In addition to that, it was also found to produce inefficacious results, from creating a general insecurity regarding political activism online for activists and the public, to radicalising and increasing harmful online political disruptions, thus, reducing overall cybersecurity and failing to deter dangerous cybercriminals and rehabilitate deviant protesters. The previous chapter also showed how governments mainly subordinate additional regulating actors through legal and political pressures to the functions and goals of the current legal regime, instead of acknowledging their autonomy and collaborating more creatively to promote more efficient and just solutions.

All these problems ultimately highlight a deficit of legitimacy, which relates to two overarching elements. The first is the lack of just and proportionate solutions mainly through violations of civil liberties and excessive punishments through vague laws and unaccountable processes. The second is the lack of efficiency, both in terms of achieving goals, such as reducing network disruptions and preventing cybercrime more generally, but also regarding overall utilitarian results, since highly punitive responses towards hacktivists can entail important personal and social harms, without achieving much in terms of compensating for disruptions or improving the security of communications and commercial transactions. These two elements, justice and efficiency, interrelate, since the lack of proportionate responses leads to less efficiacious results, such as the propagation of more disruptive behaviours by hacktivists, which in turn justifies harsher crack-downs from the authorities, with this mutual radicalisation impacting society more generally, both in terms of the exercise of civil liberties but also in terms of security online. The solutions suggested here will thus focus on remedying the highlighted legitimacy deficits by engaging with all interested sides and will induce more symbiotic methods and tools. The next section will provide some criteria for assessing legitimacy and will discuss the necessary processes for facilitating more legitimate regulatory solutions in general and for hacktivism in particular.

1. The need for different regulatory perceptions

1.1 Identifying the elements of legitimate regulation

The coerciveness of the current regulatory structure and the analogous reactions of hacktivists demonstrate the deficit of legitimacy, since, as Freeman argues, legitimate decisions are usually accepted by the public without the need for coercive measures.[1] As seen with the current treatment of hacktivism, apart from opposing user norms, such as free exchange of information, privacy and freedom of political expression, in many cases the measures have been disproportionately punitive, ineffective in promoting the aims of security and crime prevention and are often reliant on unreviewed discretionary decisions, either by prosecutors or private intermediaries. Consequently, if one would like to promote more appropriate solutions, it is necessary to identify criteria for assessing legitimacy in more detail.

Freeman's linking of legitimacy to public acceptability is discussed in relation to law-making in cyberspace, where Reed argues that in order for laws to be considered legitimate they would have to either be consistent with established user norms, or at least, be able to

[1] Jody Freeman, 'Real Democracy Problem in Administrative Law' in David Dyzenhaus (ed), *Recrafting the Rule of Law* (Hart Publishing, Oxford 1999) 335.

command the respect of citizens, which would involve demonstrating certain qualities.[2] According to Reed, these qualities are, the promotion of valuable social aims, the reasonableness of complying with them, feasible enforceability and also the production of the rules by a legal authority.[3]

Similarly, yet on a more general basis, Baldwin attempts to formulate a process for developing legitimate regulatory solutions by identifying five criteria for assessing legitimacy. These are: efficiency; the existence of a legislative mandate from the democratically elected state organs; accountability; the reaching of decision through fair and open procedures of due process; and the basing of the solutions on objective expertise.[4] As he argues, irrespective of the multiple, often conflicting, political views that might have different focal values regarding legitimacy, there are certain principles, such as those he identifies, that constitute a common ground on which discussions and assessment of legitimacy could, at least, be based.[5] Baldwin highlights the crucial need when developing regulatory suggestions, to maintain a balance between the legitimising criteria, always taking into account the concepts of legitimacy that other affected parties might have, which could lead to the solution being considered ultimately illegitimate and opposed if the stakeholders' views are disregarded.[6] These required compromises regarding the development of legitimate solutions inevitably portray the relativity inherent in assessments of legitimacy when regulating, where legitimacy can never be perceived as an absolute condition.[7] Creating justifiable regulatory responses is, thus, also a contextual process that should take into account multiple elements of justifiability and also the particular context to which the solutions relate, in order for regulators to take the particular expectations of all involved parties into account. Finding ways to balance the above legitimacy criteria in existing and new processes where many parties interact is, thus, crucial for shaping appropriate alternatives and improving existing measures. Let us then see how the process of increasing legitimacy within a multi-actor environment could be achieved.

[2] Chris Reed, *Making Laws for Cyberspace* (Oxford University Press, Oxford 2012) 17-26.
[3] ibid 20-26.
[4] Robert Baldwin, *Rules and Government* (Clarendon Press, Oxford 1995) 41-6.
[5] ibid 52-3.
[6] ibid 55-6.
[7] ibid 48-54.

1.2 Balancing multi-actor regulation and the need for symbiosis

The previous chapter demonstrated that additional actors beyond the state are engaged in the process of regulating hacktivism, highlighting the impossibility of regulating an activity solely through commands and sanctions. However, it simultaneously unveiled how state-produced rules, symbolisms and political demands influence, and even subordinate, additional actors, such as private online companies, to the dominant dictates of a 'command and control' regime and, thus, reduce the initiatives and active contribution of the rest of actors that also have regulatory potential.[8] Subordination to hierarchical demands, though, effectively negates the potential benefits of multifaceted regulation, such as decentralisation of power and increased accountability, more informed and democratised decision-making and more efficient, specialised enforcement.[9] Cooperation between stakeholders is even more important in the current era, where interconnectivity and globalisation make problems pervasive and important for all sides, rendering regulatory challenges irresolvable by isolated, single-actor efforts.[10] Therefore, we first need to see how decentralising regulation and decision-making could be realised in a balanced way, where all parties participate in producing more legitimate results and reducing conflicts.

Although additional actors, such as ISPs or civil society organisations, and tactics, such as technological filters, have been introduced in regulating online activities, there is a difference between arguing for the need for multi-actor regulation and actually producing a functional balance, since regulators often have conflicting methodologies and goals that make regulatory collaboration and progress difficult.[11] The suggestion of multi-actor regulation is not a panacea by itself, since it could end up in an undesirable smorgasbord, allow implicit regulation by incumbent actors through subordination of weaker actors or even involve alliances between actors to marginalise other factions.

[8] See Ch 4, Part 4. The role of private actors.

[9] Julia Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 3-4.

[10] Mathias Klang, 'Disruptive Technology: Effects of Technology Regulation on Democracy' (DPhil, Goeteborg University 2006) 20.

[11] Andrew D. Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge London 2007) 25, 27-8; Klang (n 10) 29.

Therefore, discussing regulatory solutions also entails managing multiple tug-o-wars between conflicting forces, in this case, factions that promote maximisation of control of information and factions that want more freedom of information.[12] However, conflicts are, also internal between different sub-actors, with public authorities, for example, being torn between satisfying the regulatory suggestions of private actors, preserving constitutional processes and/or giving in to populist influences. Hacktivists also have their philosophical and tactical internal tensions which influence their self-regulation and their reactions to external influences, despite their prima facie declarations of altruistic goals of promoting justice, fairness and democracy.[13]

The inevitability of conflict is further explained by the theory of 'autopoiesis', which perceives society, as separate systems that are self-referential, closed normatively, but cognitively open and are constituted by many subsystems that themselves self-define meaning and create unique identities.[14] This means that even though systems produce their own norms, structures and procedures, which they recognise as valid, through their cognitive openness, they can observe other systems and be influenced by them indirectly.[15] It appears that the cognitive openness of systems can gradually relax their strict autonomy, since systems need to relate to other systems and actors if they ever were to influence the regulatory environment and exert regulatory power upon other actors/systems.[16] Consequently, regulation takes a more cooperative, developmental form, being expressed as the co-evolution of the various subsystems, which happens through the indirect influence they exert on each other.[17] Contemporarily, this mutual co-evolution is further reinforced by the new technologies which have made information and interactions between actors much more immediate due to the minimisation of distance and maximisation of communication speeds.[18] Therefore, actors can share their views and communicate their approval or disaffection towards regulatory suggestions and

[12] See Ch 2, Part 1.4 The shifting power balance in cyberspace

[13] See different factions of Anonymous in Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism.

[14] Julia Black, 'Constitutionalising Self-Regulation' (1996) 59 The Modern Law Review 24, 44; Murray (n 11) 244. Much like the legal system produces and reinforces its norms and structures through its legal acts, corporations define their norms and structures through market policies, while online users and hacktivists shape their own norms and ways of communicating and acting, demonstrating their tendency for a prima facie autonomy.

[15] ibid.

[16] Gunther Teubner, *Law as an Autopoietic System* (Blackwell, Oxford 1993) 71.

[17] ibid 61; Murray (n 11) 245.

[18] Manuel Castells, *Communication Power* (Oxford University Press, Oxford 2009) 34-5.

interventions of other actors with more immediacy and, thus, accelerate and better support the processes of cognitive interaction between regulators.

The creative, deliberative interaction between multiple stakeholders thus reinforces their developmental process by inducing each actor to reconsider their approaches after documenting the norms and function of other actors and using the acquired knowledge to develop more generally acceptable regulatory suggestions.[19] Teubner argues for indirect regulatory interventions because he believes that direct interventions/impositions of one system upon another, considering their normative differences, are bound to lead to three different conditions: the indifference of the 'target' system to the intervention, the destruction of the 'target' system itself, or the destruction of the intervening system.[20] As seen throughout the thesis, especially the direct interventions on hacktivists for enforcing cybersecurity norms have indeed caused disregard to restrictions and radicalisation or even the gagging of the more moral protesters. Consequently, reducing the directly confrontational character of regulatory tools and methods employed will be consistent with the need for more co-evolutionary, indirect co-regulation, where actors will regulate themselves in accordance with indirect influences by others and will subsequently also indirectly impact on others. As Teubner argues, through the combination of the processes of developing internal norms and of interfering with other systems that indirectly impose reciprocal restraints to law, the law regulates society by regulating itself.[21]

Murray suggests that creative interactions between regulating actors could lead to more acceptable regulation and less conflict by promoting the notion of 'symbiosis'. He develops his theory also based on autopoiesis, which he applies to cyberspace interactions, considering every stakeholder a subsystem in the regulatory processes.[22] Symbiotic theory argues that 'the best regulatory model is not one built upon an active intervention into the settled regulatory environment, the result of which is likely to be extremely disruptive, rather it is one that harnesses, as best as possible, the relationships already in place between the actors.'[23] Communication between actors here plays a crucial role, with

[19] Julia Black, 'Constitutionalising Self-Regulation' (n 14) 44-5.
[20] Gunther Teubner, 'Juridification: Concepts, Aspects, Limits, Solutions' in Gunther Teubner (ed), *Juridification of Social Spheres: A Comparative Analysis in the Areas of Labour, Corporate, Antitrust and Social Welfare Law* (De Gruyter, Berlin 1987) 3-48.
[21] Teubner, *Law as an Autopoietic System* (n 16) 65.
[22] Murray (n 11) 243-5.
[23] ibid 243-4.

regulators gathering information from the various stakeholders and making viable regulatory suggestions based on the information gathered through the processing of constant feedback expressed by the other actors through compliant or disruptive interventions in a closed-loop system.[24] The minimisation of conflict and the simultaneous effort for gradual compromises are very important for regulating hacktivism as a phenomenon arising purely as a consequence of regulatory conflicts online. Therefore, symbiosis seems to more appropriately describe the way multi-actor regulation could work in a regulatory environment that already has an established modus operandi (criminal justice system), but is also moderated by various other actors (private corporations or user communities) and is rife with conflict-inducing, constant interactions. The model of symbiosis and gradual, multifaceted change is also consistent with hacktivism, which is a symbolic, publicising and sensitising tactic that is usually doneperformed to bring change by setting smaller changes in motion and not through openly demanding an immediate radical shift of paradigms.

An important aspect of symbiosis is also the active role of the regulatees. Regulation in the network does not have passive regulatees, so, in addition to being regulatees, hacktivists are indeed a regulating force within the wider struggles of regulating speech and privacy online, thus also impacting on how they are eventually treated. Essentially, they influence their own regulation through self-regulation and the pressures they exercise on the more traditional public and private regulating forces in the same way that Teubner discusses about law.[25]

Before proceeding to analyse the potential solutions in more detail, it needs to be made clear that the following regulatory suggestions inevitably entail a certain degree of optimism and patience. They are made with the knowledge that parts of what is suggested, although potentially consistent with basic principles of law and accepted social values, could prove challenging to apply in the current security-based climate and could only happen, as discussed through indirect slow processes of interactions between stakeholders.

Despite some suggestions going against the current regulatory trends, the symbiotic theory of indirect, gradual co-evolution shows us that, even if initially suggestions might appear controversial, through symbiotic process regulators might gradually become more

[24] ibid 247-8.

[25] See text to (n 21).

accepting. Indeed, there have been cases where suggestions that were initially considered extraordinary and impossible have gradually become tested and partially accepted. For example, restorative justice solutions had been considered difficult to promote in theory and practice, yet steps have been taken gradually towards that direction with interesting results.[26] Moreover, the acceptance of civil disobedience, even though initially condemned by theorists such as Hobbes, has gradually become morally acceptable by theorists that build on Hobbesian notions, such as Habermas and Calhoun.[27]

Shaping more appropriate solutions is a slow process of acquisition of information and transforming it to knowledge, of deliberation and gradual integration of regulating contributions from all the actors engaged in the regulatory processes and ultimately based on achieving common understandings and promoting legitimacy. Inevitably, regulatory suggestions will not follow a traditional structured model, but will appear as a network of constant modifications and interactions between the various actors, methods and tools that influence the regulation of hacktivism directly or indirectly. Let us begin by discussing how to improve criminal justice perceptions and processes.

2. Improvements in the criminal justice system

According to the adopted symbiotic model, the starting point will be to discuss changes that relate to the established approach that focuses on prosecutions and sanctions based on cybercrime laws. Irrespective of the many deficiencies identified so far in the thesis, particularly for issues of public interest, such as delinquency, the criminal justice system still maintains its importance as a process that regulators are accustomed to employ and also as a source for normative dictates and processes for guiding regulatory choices.[28] Moreover, the introduction of the Internet into already established, state-focused regulatory perceptions makes it very hard to perceive regulation of criminality online as independent

[26] For the gradual introduction of restorative justice processes into mainstream criminal justice practice see: Andrew von Hirsch et al. (eds), *Restorative Justice and Criminal Justice: Competing or Reconcilable Paradigms?* (Hart Publishing, Oxford 2003); John Braithwaite, *Restorative Justice and Responsive Regulation* (Oxford University Press, Oxford 2002).

[27] Juergen Habermas and Martha Calhoun, 'Right and Violence: A German Trauma' (1985) 1 Cultural Critique 125.

[28] Brownen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, Cambridge 2007) 95.

from already existing norms, established laws and judicial decision-making processes.[29] As Goldsmith and Wu argue, even if our lives are dominated mostly by social norms and symbolisms, market influences or even technological measures in cyberspace, rather than laws, an underlying system of territorial government and physical coercion is also needed in order for these controls to function properly.[30]

The importance of the legal system, even for nodal regulatory structures, does not just lie in the shaping of social behaviours, but also in its usefulness as a tool, which institutionalises security and justice values, and normally provides procedures, if not paradigms, of accountability for other regulating forces.[31] As Lessig argues, in a society where corporations define code and influence behaviours online, state-originating controlling mechanisms can offer negative and positive normative and practical examples, and infuse novel regulatory developments with important values.[32]

Consequently, the inclusion of the governmental agencies and legal processes in regulatory structures could prove to be, not just unavoidable, but also very useful, as it could highlight the areas where regulatory suggestions practically require supplementary efforts or alternative solutions and actors. The first stage of changes to be introduced here is the enabling of law and law enforcement to promote a symbiotic interaction and to progressively integrate more interactive, just and efficient processes in the functioning of the criminal justice system.

The crucial question is to identify the elements and the steps that would enable the gradual turn towards symbiosis and increased legitimacy within the current cybercriminal legal framework. We can initially identify two ways for realising these processes. One would be to promote the introduction of clearer definitions and harmonised approaches to particular activities. The other way is the promotion of education of the public and of those creating and enforcing the laws and processes of the criminal justice system regarding new technologies and hacktivism, its perpetrators, benefits and potential risks.

[29] Suart Biegel, *Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace* (The MIT Press, London 2003) 52.

[30] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, Oxford 2006) 181.

[31] Morgan and Yeung (n 28) 228, 236.

[32] Lawrence Lessig, *Code v.2.0* (Basic Books, New York 2006) 77-8.

2.1 The need for clear definitions and harmonised approaches

Regulators wanting to overcome the uncertainty and vagueness of cyberlaws regarding their applicability on hacktivism will have to find some generally applicable and commonly acceptable interpretive principles that will reduce the indeterminacy and overlapping of the current provisions. As Braithwaite has argued, reliance on more general principles that will be consistently employed can provide us with better solutions than reliance on specific laws.[33] As he submits, regulating solely through binding rules is problematic when the definitions of the regulated activities are contested, especially those that entail economic and technological changes that challenge given norms and which could both be proscribed or allowed.[34] In the normatively and practically complex cases of hacktivism, adopting specific principles defining what behaviours should be considered dangerous or prosecutable in relation to online political activities could provide useful guidance regarding the applicability and the mode of application of cybercrime provisions to hacktivist tactics. For example, the issue of unauthorised access and reckless damage and the relation to virtual sit-ins[35] will have to be clarified based on the goals that the legal regime aims to achieve and not on random interpretations by various courts. This will not only provide a nationally consistent approach, but will also facilitate the adoption of general principles and criminalisation rationales that other jurisdictions have established or could establish, thus facilitating harmonised approaches.

As is apparent, therefore, clarity and legal certainty cannot come from the promulgation of an increasing amount of overlapping cybercrime laws, especially in common law regimes where courts can partly function as law-makers and provide their own definitions. There ought to be declared aims and principles, as to which the goals that the legislation is trying to achieve are, as can, for example, be extracted by communal efforts such as the Cybercrime Convention,[36] in order for interpretations to have a clear and common starting point and which eventually will hopefully also achieve increased harmonisation. Harmonisation will, however not be achieved by creating identical legal provisions amongst

[33] See John Braithwaite, 'Rules and Principles: A Theory of Legal Certainty' (2002) 27 Australian Journal of Legal Philosophy 47.
[34] ibid 55.
[35] Ch 4, Part 3.3.3 Unauthorised access and intentional damage.
[36] Council of Europe, 'Convention on Cybercrime' (ETS No. 185; Budapest, 2001).

states, but by making certain that the aims behind those provisions are consistent with generally accepted cybersecurity goals in the same way that the, largely ignored by the UK and US, Council of Europe Cybercrime Convention has attempted to do by providing general guidelines and suggested safeguards in framing cyberoffences.[37] Defining a place for hacktivism within these debates will, thus, become easier when the basic principles of criminalisation in cyberspace are identified and followed without being explicitly designed and imposed. As Astier submits, 'while unification implies precise rules to which the states are obliged to conform in an identical way — applying the principle of the hierarchy of standards — harmonization implies a weakening of this principle, imposing only a reconciliation on the basis of common principles'.[38]

As Dworkin suggests, focusing on principles, rather than strict rules, also reinforces a - much desired in the case of ECD - flexibility for the adoption of specific, contextual solutions, since it allows for conflicting principles to be weighed in order to produce the best result possible according to the social importance of the interests conflicting each time.[39] Moreover, principles, being fewer, shorter and simpler than detailed laws, could more effectively promote broader discussions regarding regulation between different actors. Reliance on often overlapping and conflicting provisions from a legal jurisdiction could hinder regulatory progress and instead generate more conflict between different jurisdictions and ways of expression, especially since rules are more influenced by the indeterminacy of language than principles.[40] Therefore, consistency in the promulgation and application of cyberlaw regarding online politics could flow from focusing on finding or highlighting commonly accepted standards, rather than by creating ever-expanding legal rules that, instead of explaining, further confuse interpretations.

2.2 Informed processes in the criminal justice system

Harmonious symbiosis between all actors would also require the obtaining of information on behalf of actors influencing the regulation of hacktivism in relation to the general

[37] ibid; see allowances and criteria for moderating liability in Title 1. See also discussion in Ch 4, Parts 3.3.1 and 3.3.2 The further criminalisation of inchoate offences.

[38] Stephane Astier, 'Ethical Regulation of the Internet: The Challenges of Global Governance' (2005) 71 International Review of Administrative Sciences 133, 139-140.

[39] Ronald Dworkin, 'The Model of Rules' (1967) 35 University of Chicago Law Review 14, 25, 27.

[40] Braithwaite, 'Rules and Principles' (n 33) 75.

dimensions and risks of cybercrime in addition to more specific hacktivism-related information regarding the ideological and tactical background and potential consequences of these groups' actions. Consequently, information gathering before any legislative, prosecutorial or judicial decision-making would be a crucial regulatory improvement.[41] Since a common deficiency of law-based regulation is the lack of information and specialised knowledge,[42] especially where the level of technological specialisation exceeds the knowledge of public officials[43] the realisation of the need of informed decisions and acquisition of specialised knowledge would be crucial for the more just, efficient and harmonious employment of the criminal justice system as a prominent regulatory tool regarding hacktivism and more generally. This could be facilitated by engaging, not just with media reporters and security firms, but also individuals that have participated in such activities and independent researchers with knowledge in the relevant areas of hacker culture, politics or cybercrime.

Through such an increase in understanding, prosecutors might also become less adversarial towards hacktivists - a change that could facilitate more balanced decisions than those seen so far.[44] The achievement of more balanced decisions will, in turn, increase the overall acceptability of potential prosecutions and will reduce tensions and polarisation between protesters and authorities, which are currently intense. The proliferation of information and specialised knowledge on hacktivism is also very important for disentangling the normative understanding of cybercrime from the negative and generalising dictates of media and large commercial entities, such as software manufactures and security and content providers.[45]

An understanding of new digital technologies would allow prosecutors and judges to consider the fact that legal norms are also produced by other actors and communities, which stretch beyond national borders, thus, supporting a need for a more cosmopolitan

[41] Julia Black, 'Proceduralisation and Polycentric Regulation' (2005) Especial 1 RevistaDIREITOGV*,* 99 <http://direitogv.fgv.br/sites/direitogv.fgv.br/files/rdgv_esp01_p099_130.pdf> accessed 16 December 2012, 109.

[42] Ch 1, Part 1.1 Defining regulation.

[43] Many critics of the inefficiencies of state regulation have focused on the capacity of private actors and more specialised agencies to better understand and have the know-how for dealing with problems that require specialised knowledge. See Black, 'Critical Reflections on Regulation' (n 9).

[44] Kenneth J. Melilli, 'Prosecutorial Discretion in an Adversary System' (1992) Brigham Youth University Law Review 669.

[45] Ales Zavrsnik 'Cybercrime Definitional Challenges and Criminological Particularities' (2008) 2 Masaryk University Journal of Law & Technology 1, 8.

viewing of Internet-related problems.[46] Moreover, education of the dimensions and implication of hacktivism would be important because judges often decide on issues with international consequences, without any consideration of their decisions' extraterritorial implications.[47] The direct implication of such a critique for courts is that judges, through their familiarisation with the nature of the phenomena they adjudicate, will gradually become more capable of assessing the knock-on effects of their decisions which are often quasi-legislative in nature. Moreover, judges will become able to shape their judgments based on an understanding of the many different sources that influence online behaviour and normative standards.[48] Increasing technological education and social discourse regarding hacktivism and the relevant political challenges could, therefore, produce more legitimate and more generally acceptable decisions.

Informed prosecutors and judges could also provide better guidance and clarifications for juries, thus making them more capable of understanding and adjudicating on the nature of online political activities. Jurors, being laypersons, are very much influenced both by the pervasive social symbols as well as the prosecutors' attitude towards the offenders.[49]The importance of education and information will also relate to the general public, since, as has been seen in previous chapters, when the public is informed about the specific details of the offences and the potential penalties, it becomes far more understanding and supportive of solutions and punishment that would be more lenient and more specific to the particular offence and offender.[50]The education provided, in order to be more effectively preventive, should thus take the form of generating informed citizens that will be able to make knowledgeable decisions, rather than the form of preaching against certain phenomena in order to discourage citizens from resorting to these.[51]

Educating the public does not just relate to having a more informed jury, but also to more informed public participation for those wanting to participate in mass-action

[46] Allan R. Stein, 'Parochialism and Pluralism in Cyberspace Regulation' (2004*)* 153 University of Pennsylvania Law Review 2003*,* 2004.
[47] ibid.
[48] ibid 2006.
[49] Ch 4, Part 2. The normative framework and its impact on hacktivism. See also Glenn Reynolds 'Ham Sandwich Nation: Due Process When Everything Is a Crime' (Legal Studies Research Paper No. 206, University of Tennessee, Tenessee 2013) <http://ssrn.com/abstract=2203713> accessed 20 June 2013.
[50] See Ch 3, Part 2.2.3 Are highly punitive sanctions for ECD utilitarian?
[51] Morgan and Yeung (n 28) 100.

hacktivism (virtual sit-ins, viruses), as well as to the prevention of unjustified moral panics from exaggerated media reports. Informing the public regarding the nature of hacktivism and the implications for the networks targeted, as well as of the potential penalties, will essentially prove more deterrent than prosecution, at least in relation to less moral incidents of hacktivism. Such public education will also reduce punitive excesses with the justification of appeasing public fears, which is commonly used as justification for legislative and executive excesses.[52]

The effort to make these changes would be crucial in preserving the legitimacy of the courts' decisions and also demonstrate that criminal justice can provide informed and appropriate decisions in relation to cyberspace phenomena. These elements would, in turn, increase compliance with the decisions and would also reduce social conflict and radical responses.

2.3 Reconsidering the focus on damage and loss and restoring the focus on culpability

Transparency, equality and more deserved penalties could also be promoted through the reconsideration of damage/loss definitions and of the processes for calculating them in computer misuse offences. By deciding to focus on losses for assessing liability and penalty extents, current laws and sentencing guidelines reflect an almost 'strict liability standard' that criminalises even benign hacking aimed at exploration and innovative uses of technology.[53] This is especially so, since the threshold of unacceptable damage is either easily reachable by low harmfulness hacktions or the damage extent is irrelevant for incurring high penalties.[54] This realisation, in addition to focusing less on culpability and mitigating circumstances, while expanding the culpable mens rea of computer offences,

[52] Ch 4, Parts 3.1 The making of cybercrime laws and 5.1.1 Prosecutorial power and the new mentality.

[53] Trevor Thompson, 'Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the White Hats under the CFAA' (2008) 36 Florida State University Law Review 537, 559-60.

[54] ibid 557; Both in the US the felony requirements, as well as the Computer Misuse Act 1990 in the UK have a small interest in the extent of damage for establishing liability and focus more on assessing damage and loss for sentencing. See Ch 4, Part 3.3.1 The focus on damage and loss and the expansion of the scope.

contrary to guidance from law commissions and guiding conventions,[55] suggests that regulators would normally have the leeway to moderate the attention on damage and loss, or at least, define it more narrowly and find more accountable ways of assessing damage and loss than just relying on victims' assessments and cybersecurity firms' predictions. The importance of these factors (loss/damage) could be moderated indirectly by introducing more inclusive and, at least, two-sided assessment processes for the damage and losses caused that would come from not only the victims, but also from protesters. More restrictive, yet adequately inclusive definitions of loss/damage could extract abstract elements from calculations relating to loss that would not be directly caused or predicted by the allegedly offensive protesters. For example, it has been suggested that the costs of re-securing should not be included in liability and punishment extent calculations, since security and the patching of systemic weaknesses are considered a given and consistently reassessed and updatable responsibility of the targets.[56] Moreover, it is suggested that reputational harms, system improvements and forensic expenses should be excluded from the general cost assessments.[57]

Establishing mitigating circumstances in the sentencing guidelines, if not the cybercrime provisions per se, could also facilitate the moderation of attention to damage and loss and renew the focus on culpability, thus allowing moral deviants to achieve more lenient penalties in accordance to their character and motivations. The US Sentencing GuideliInes provide very few guidelines regarding motive, especially for mitigation.[58] In the UK, even though motive is part of the culpability assessments which influence the ultimate assessments of harm,[59] the sentencing guidelines consider greed motives as the base motive for committing a criminal offence and then designate aggravating circumstances

[55] Ch 4, Parts 3.2 The applicable unauthorised access offences and 3.3 The dominating provision of computer damage.
[56] Reid Skibell, 'Cybercrime and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act' (2003) 18 Berkeley Technogy Law Journal 909, 941-4;
[57] Jennifer Granick, 'Faking It: Calculating Loss in Computer Crime Sentencing' (2005) 2 A Journal of Law and Policy 207*,* 208, 228.
[58] United States Sentencing Commission, '2011 Federal Sentencing Guidelines Manual' <http://www.ussc.gov/Guidelines/2011_Guidelines/Manual_PDF/index.cfm> accessed 21 June 2013.
[59] See Section 1.17 Harm must always be judged in the light of culpability. The precise level of culpability will be determined by such factors as motivation, whether the offence was planned or spontaneous or whether the offender was in a position of trust. Sentencing Guidelines Council, 'Overarching Principles: Seriousness' (2004) <http://sentencingcouncil.judiciary.gov.uk/docs/web_seriousness_guideline.pdf> accessed 21 June 2013.

regarding various kinds of malign motives, such as racism or sexism.[60] However, there is no provision in the guidelines for a mitigating factor based on socially considerate motives. Considering the impact that motive seems to have, on at least the extent of punishment – given that motivation does not feature in the decision of whether an act was criminal, including such elements in the sentencing guidelines regarding altruistic motives could balance the motive-related factors which currently primarily involve aggravating factors. This could also be achieved by paying more attention to elements such as benign motives, thus, facilitating distinctions between morally- and egotistically-motivated cyberdeviants. Allowing evidence of motive and making it a more active element in the judicial process could also increase the legitimacy of the sentencing decisions. This will be due to the fact that even convicted protesters will feel their demands have, at least, been expressed and considered and will also give another forum for protesters to use the courtroom and the consequent media attention in order to make their case more widely known.

Another way that attention could be given to motives is by allowing juries to hear a defence of necessity for cases of online political law-breaking - something which has been extensively attempted in cases of offline CD.[61] There are, however, as seen in the previous chapter many hurdles to using this defence for political protests, both in terms of applicability requirements, but also of a more political nature.[62] Applying such a defence to hacktivism will be harder than offline cases, requiring a broader interpretation of the defence's requirements. Despite the difficulties in satisfying the criteria for applying necessity and the explicit ban on indirect CD established in *US v Schoon,*[63] the fact that there have been cases where the defence has been allowed, such as *People v Gray*[64] and others,[65] makes it plausible to discuss the prospect of allowing necessity for hacktivist actions.

The benefits from the prospect of allowing necessity are two-fold. First, allowing the defence will further legitimise any potential penalty, since the sanctioning will be a result of

[60] See also Sentencing Guidelines Council, 'Magistrate's Court Sentencing Guidelines: Definitive Guideline' (2012) <http://sentencingcouncil.judiciary.gov.uk/docs/MCSG_Update9_October_2012.pdf> accessed 21 June 2013.
[61] Ch 4, Part 5.2.3 The role of the jury.
[62] See discussion in ibid.
[63] 22 Ill.971 F.2d 193 (9th Cir. 1991)(*Schoon).*
[64] 150 Misc. 2d 852 (N.Y. Co. 1991)(*Gray*).
[65] Ch 4, Part 5.2.3 The role of the jury.

the jury's assessment of the justifiability of the protests. Considering that the jury reflects the public sense of justice,[66] any punishment that would be imposed by them would be more acceptable for protesters, rather than the decision being solely reliant on a judge. Secondly, the potential for employing such a defence would increasingly induce protesters to abide by certain moral standards and principles in order to satisfy the criteria for allowing the defence and, thus, have an increased chance of reducing, if not totally avoiding, liability. Even if the defence is not accepted in full for ECD, its examination and the introduction of evidence it will entail regarding the political motives of protesters will give the criminal process an increased feeling of fairness, allow more political deliberation in relation to these political cases and increase self-regulation by hacktivists.

The previous chapter discussed how the US Ninth Circuit court has articulated a four-pronged evidentiary test that defendants have to satisfy for the jury to hear their defence and I argued that CD and hacktivism might be challenged to satisfy these criteria as they have been interpreted.[67] The elements are (a) that the defendant chose the lesser harm of the two (b) the law-breaking was meant to prevent an imminent harm, (c) he reasonably anticipated a causal relation between the law-breaking and the harm avoided and (d) there was no other legal alternative to breaking the law. All requirements of the necessity defence demand that a court makes assessments of reasonableness, requiring an objective reasonableness of the protesters' beliefs.[68] Contextual elements that might have influenced the judgment of reasonableness on behalf of the protesters will also feature in the assessment of this objectivity.[69] Let us then see whether these elements could be interpreted in ways that would be satisfiable by hacktivists.

The first criterion is easily satisfiable, since the harms protested against are usually much more important than a website disruption. The first difficulty for protesters arises from the requirement that protesters maintain a reasonable belief of the necessity of their actions for averting the harm protested against. Protesters would satisfy this element of the defence, if they can convincingly argue that they reasonably considered their actions would

[66] ibid.

[67] *US v Dorrell,* 758 F.2d 427, 430-31 (9th Cir. 1985) cited in *US v Aguilar*, 883 F.2d 662, 693 (9th Cir. 1989).

[68] John A. Cohan, 'Civil Disobedience and the Necessity Defense' (2007) 6 Pierce Law Review 111*,* 125.

[69] ibid.

contribute to averting the harm.[70] However, with indirect CD that operates only as a trigger of events for preventing harms or as part of a more concerted effort towards change, rather than a directly averting act, proving the reasonableness of a belief of necessity can be more challenging.[71] Most courts do not accept the reasonableness of a belief in a causal link between the symbolic protest and the injustice to be prevented or stopped.[72] More particularlyin *Schoon,*[73] the court established a rule of causality, where the legal violation should by itself bring the change in policy. Therefore, this conflict between the legal requirement and the realistic way that causally relevant protests are assessed should be reconsidered in order to reflect the scale of injustices protested and the scale of the causal political effort needed.

In the case of hacktivism, where the online and symbolic nature of the protest might make it even more indirect and causally distant in relation to the prevention of the harm, the courts' denial will seem even more justified. A solution here could be to perceive the online protests as a reasonably necessary part of a sequence of acts that would be considered crucial for actually preventing the political harm in question - something potentially supportable, but certainly not easily acceptable. Commentators have considered merely symbolic acts like draft card-burning to actively and causally contribute to maintaining and furthering rational discussion, attracting people in the debates on serious policy issues and eventually promoting a review of policies by the government.[74] Accepting such a rationale could mean that hacktivist protests could potentially be seen as causally contributing to the prevention of the harm. For example, in the case of Anonymous' operation Payback, during which they organised sit-ins to protest the freezing of Wikileaks

[70] Matthew R. Lippman, *Contemporary Criminal Law: Concepts, Cases, and Controversies* (Sage Publications, London 2010) 256.

[71] Lippman (n 70) 256; See *US v Maxwell,* 254 F.3d 21 (1st Cir. 2001)(*Maxwell*) where such a rationale was accepted.

[72] Matthew Lippman, 'Civil Disobedience: The Dictates of Conscience Versus the Rule of Law' (1986) 26 Washburn Law Journal 233, 246-8; see *US v Kroncke* 459 F.2d 697 (8th Cir. 1972); *US v Marley,* 549 F.2d 561 (8th Cir. 1977)(Marley); See *Maxwell* (n 71) where reasonableness was accepted. Bernard D. Lambek, 'Necessity and International Law: Arguments for the Legality of Civil Disobedience' (1987) 5 Yale Law & Policy Review 472*,* 477; The court in *Gray* (n 64) has accepted such a prospect.

[73] *Schoon* (n 63).

[74] Ted Finman and Stuart Macaulay, 'Freedom to Dissent: The Vietnam Protests and the Words of Public Officials' (1966) Wisconsin Law Review 632*,* 682; James L. Cavallaro, 'The Demise of the Political Necessity Defense: Indirect Civil Disobedience and United States v. Schoon' (1993) 81 California Law Review 351, 374-5.

donations, protesters believe that the Anonymous' operation and the consequent bad publicity and political pressure led to the reactivation of the Wikileaks accounts.[75]

The imminence requirement might also prove a second challenging aspect for hacktivists to satisfy. Although in many cases, like environmental protests, the ultimate goal might be the prevention of a life-threatening harm beforehand, such as a nuclear disaster, courts will often demand imminence,[76] even though most acts of CD and ECD could relate to long term policy decisions or the avoidance of future harms.[77] The rationale behind imminence is that, usually, if there is time for the harm to happen, legal means will usually be available.[78] However, modern harms could be of a nature or scale that cannot be considered imminently preventable and would instead require a long term policy-change campaign in order to prevent or further minimise the possibility of the expected or an ongoing harm.[79] The court in *Gray* accepted that, if the harm is provably and reasonably serious and ongoing or of a nature that would require the lesser evil to happen well in advance, the criterion of imminence should be considered satisfied.[80] As for the criterion of direct efficiency of the protest to the prevention, the same court argued:

> An inflexible test allowing for no inquiry into the circumstances and events surrounding the formulation of a defendant's belief, while imposing an after- the-fact requirement of an immediate relationship, constitutes a rule of per se unreasonableness, whereby a defendant who fails is held as a matter of law not to have reasonably believed in the efficacy of his action[...]Penalizing them because a

[75] Charles Arthur 'Inside 'Anonymous': Tales from within the Group Taking Aim at Amazon and Mastercard' *(The Guardian Technology Blog,* 13 December 2010) <http://www.guardian.co.uk/technology/blog/2010/dec/13/hacking-wikileaks> accessed 19 December 2012.

[76] See *Marley* (n 72); *US v Berrigan,* 283 F. Supp. 336 (Dist. Court, Maryland 1968)(*Berrigan*); However in *Gray* (n 64) the court accepted a broader notion of imminence without requesting immediacy. Cohan (n 68) 132-3.

[77] Tammy A. Tierney, 'Civil Disobedience as the Lesser Evil' (1988) 59 University of Colorado Law Review 961, 974; See Lippman, 'Civil Disobedience (n 72) 246-8; *Marley* (n 72).

[78] George P. Fletcher, *Basic Concepts of Criminal Law* (Oxford University Press, New York 1998) 135.

[79] According to Hegel, for seriously unjust and harmful conditions, necessity could be perceived not as being of an imminent, momentary nature, but as a long-term situation. Mark Tunick, 'Hegel on Justified Disobedience' (1998) 26 Political Theory 514, 528.

[80] *Gray* (n 64).

> result reasonably expected did not actually occur immediately following their action, would be contrary to the purposes of the necessity defense.[81]

After all, the expectation of necessity does not also mean 'sufficient to prevent the harm' and, therefore, certainty of prevention on behalf of protesters should not be required. If imminence is interpreted more broadly in relation to the nature of the harm, the expectation of imminence could become more flexible in order to at least allow protesters to present their case to a jury.

The third criterion that is problematic is the exhaustion of legal alternatives, ensuring that the defence will not justify harmful, illegal acts, when there are less harmful, legal routes of amelioration. However, as discussed in chapter two,[82] the actual existence, accessibility and efficiency of legal measures will often be questionable, since the scale of the harms protested could be of a global nature, eliminating any chance of access of citizens to legal alternatives or ensuring that legal alternatives might have been exhausted without success. Again the Wikileaks example, where the court's decision was made more than a year after the decision of Visa not to process donations is characteristic of how waiting for legal alternatives to be exhausted could prove problematic for the cause of the protest. CD and hacktivist protests could even aim to influence the initiation or result of a legal measure taken by drawing attention to the specific political challenge and sensitising the public and its representatives in Parliament. Protests before the passing of extreme austerity measures in Greece are a characteristic example of a pending legitimate decision that protesters would like to influence with legal and civilly disobedient means. Consequently, courts ought to reconsider the concept of exhausting legal alternatives in relation to the accessibility of these alternatives to interested parties and the potential success of these measures.[83] After all, the Model Penal Code provision of necessity has not included imminence or the exhaustion of legal alternatives. If we considered that to be indicative of the basic elements of necessity, one could argue that added criteria could be reconsidered or applied in a more relaxed way in order to accommodate the realities of contemporary politics. The same arguments could be applicable for the higher law defence,

[81] ibid 869-70.

[82] Ch 2, Part 3.5 Last resort.

[83] See also Ch 2, Part 3.5 Last resort.

which is also based on similar concerns of necessity, causal nexus, imminence and exhaustion of legal alternatives.[84]

A last question to be answered when allowing these defences is the political question of whether allowing the jury to decide on whether a protester has the right to protest against a governmental policy would render the courts a substitute for the legality of legitimately passed governmental decisions. Undeniably, it would be very dangerous to a legal system if juries were allowed to render an official political decision made by the state's representatives illegitimate through their acquittals for necessity; a main reason the defence has not been accepted often.[85]

Although, such an argument potentially makes sense for parliamentary acts, it would be non-applicable when protesters target private party policies that have an impact on the general public, such as environmentally destructive policies of private chemical companies which are increasingly the causes of protests, or decisions that have not been properly deliberated by the executive or the legislature.[86] Furthermore, the concern of political pre-emption relates to protesting through direct violation of the law protested – thus, putting courts in a position to decide on the validity of the law and condemn or render the law invalid and acquit the protesters.[87] Consequently, the 'political question' issue would not be applicable to hacktivism as a form of indirect CD. As for the higher law defence, courts have also allowed protesters to present evidence based on the existence of a higher law violation, when arguing that specific state policies were illegal, and protesters were eventually acquitted.[88] The court in *Vt. v McCann* also explicitly argued that an issue protested does not take the dimension of a political question merely because it relates to social policies or issues of public interest, but because the protester offers evidence as to the illegality of the policy, rather than a more abstract criticism of its appropriateness or wisdom.[89] Such an issue of illegality was considered appropriate for assessment by the

[84] Ch 4, 5.2.3 The role of the jury.

[85] Lippmann 'Contemporary Criminal Law' (n 70) 219.

[86] See for example: Greenpeace, 'Bhopal Protests Move Online' (*Greenpeace*, 10 March 2003) <http://www.greenpeace.org/international/en/news/features/bhopal-protests-move-online/> accessed 24 October 2010.

[87] *Gray* (n 72) 857.

[88] See *Mass. v Carter*, No. 8745-JC-0091A (Dist. Court, Hampshire County, Mass. 1987); *Vt. v McCann*, No. 2857-7-86 (Dist. Vt. 1987), *reprinted in* 44 GUILD PRAC. 101 (1987)(*McCann*). See details in Cohan (n 68) 170-2.

[89] McCann (n 88) 109-110.

judiciary since otherwise the executive would be above the law and the defendant was exonerated based on this defence.[90] Furthermore, as the court in *Gray* has argued, if the protest relates to a view that has also been established through legislation, such as the reduction of air pollution, there will not be an issue of legislative pre-emption, since protesters will be supporting legally established social goals and principles.[91]

If hacktivist protesters have similar bases to their protests or target private policies, then the political question concerns should not pose an issue for being allowed to employ these defences. This subsection does not advocate that the defences be allowed in every instance. Instead, it is envisaged that use of this defences would be accepted in select cases, based on the protesters satisfying the broadened standards, as discussed in this subsection. Even if not ultimately successful, the opportunity for the protesters to present their cause and motives to the jury, the courtroom audience and the wider audience through media reporting, could induce more understanding responses in the cases where protesters actually make an effort to act morally, encourage protesters to act so and also increase political deliberation regarding established political issues and injustices.

2.4 Offering safe harbours for cooperative behaviours of offenders

An alternative suggestion for reducing harmful political disruptions online and also, actively improving overall collaboration and cybersecurity is the promulgation of incentives and rewards for commendable performances.[92] Regulatory tactics that relate to the provision of incentives have been commonly employed, mostly in the form of financial incentives provided to companies in exchange for compliance and cooperation.[93] However, even within the context of the criminal justice process, one could introduce incentives that will have an impact on hacktivism and will not be linked to financial incentives, but to penalty mitigation or exoneration offers. Such rewards could induce protesters to behave in less

[90] ibid; See also *Vt. v Keller*, No. 1372-4-84 (Dist. Vt., 1984); *Chi. v. Streeter*, No. 85-108644 (Cir. Court, Cook County, Ill. 1985); *Ill. v Jarka*, No. 002170 (Cir. Court Ill. Apr. 15, 1985) *reprinted in* 42 GUILD PRAC. 108–10 (1985). In these cases, the defendants were acquitted regarding protests against US politics in South America, or, in the case of Streeter, of the illegal segregation policies of the South Africa government.

[91] *Gray* (n 72) 858.

[92] Martin Krygier, 'Ethical Positivism and the Liberalism of Fear' (1999) 24 Australian Journal of Legal Philosophy 65, 89.

[93] Morgan and Yeung (n 28) 82.

harmful and more legitimate ways, while also promoting more lenient, specialised penalties and cooperation between parties that might, in principle, have common concerns, such as the protection of consumer privacy. For example, hacktivists often hack in order to demonstrate lax security in companies and, unless their intrusions are accompanied by misuse of the information obtained through the security holes identified, their acts should not be considered worthy of punishment, if the sole aim is the exposure of a company's disregard for user security.[94] Unfortunately, the current system attempts to punish such hackers as felons, rather than acknowledge the potential benefits from highlighting these breaches and allow overall improvements to security by inducing hacktivists to share the details of the exploits.[95]

Solely prohibitive measures do not educate citizens to behave responsibly online and to avoid or reduce damaging or loss-inducing behaviours that could increase their penalties. Instead, protesters, as has been seen, are often induced to resort to methods to avoid identification and liability for their law-breaking, for example, by masking their identities. The opportunity to motivate citizens to be responsible, when hacking for socially beneficial ways would, thus, operate more efficiently if political hackers finding security problems knew they will not be prosecuted as hardcore criminals. If sharing information in relation to the security breaches could be employed as an incentive in exchange for mitigation of penalties or even non-prosecution, hacktivists might be even more willing to collaborate with the authorities or the companies involved in order to accelerate the efforts to patch security holes and will potentially avoid masking their identities or exposing the information online in order to induce the publicisation and patching of the security flaws.

[94] Hacktivist groups have also often supported crime prevention purposes, such as exposing software vulnerabilities or monitoring and exposing child pornography websites and offenders. See Ch 1, 2. Hacktivism: Definitions, groups and tactics; Violet Blue 'Anonymous Attacks Child Porn Websites and Publish User Names' (*ZDnet Blog,* 21 October 2011) <http://www.zdnet.com/blog/violetblue/anonymous-attacks-child-porn-websites-and-publish-user-names/757> accessed 19 February 2012.

[95] For example a Auernheimer, a self proclaimed troll, was sentenced to 41 months in prison for having obtained email accounts of users by taking advantage of a network flaw in the AT&T network. See US *v Auernheimer*, Criminal No.: 2:11-cr-470 (SDW) (Dist. Court, New Jersey 2013); Another alleged member of Anonymous, who claims to have helped expose two rapists in the Steubenville, Ohio rape case through legally obtaining and publishing online information is threatened with high penalties as well based on charges of hacking into a website to post such materials, an act for which another collaborating hacker has claimed responsibility. See Nancy Goldstein, 'Steubenville's Tangled Web of Injustice' (*The Guardian,* 12 June 2013) <http://www.guardian.co.uk/commentisfree/2013/jun/12/steubenville-tangled-web-injustice> accessed 21 June 2013.

If such safe harbour collaborations become pervasive, regulators could also avoid punishing hacktions, such as web-defacements, re-directs and virus distributions. The precondition would again be that the security weakness used for realising these protests is revealed to the website administrators, or are publicised generally perhaps with ways to patch these problems, if they relate to weaknesses inherent in commonly used software. Safe harbour provisions would thus be based on avoiding the harsh punishment of morally motivated users, while increasing overall security by providing information about network weaknesses and also allowing the opportunity for the protest to take place.[96]

The provision of such mitigation/exoneration opportunities could be reliant either on prosecutorial discretion or even more explicitly established as a mitigating circumstance in sentencing guidelines. The consistent employment of these safe harbour opportunities would also shift the focus from damage and loss to the motivation of protesters and their ultimate result regarding cybersecurity. Consequently, the protesters' restorative reaction would establish a defence mitigating their culpability. Promoting safe harbour provisions for ethical, collaborative hackers would serve the purpose of increasing overall security by preventing more harmful compromises in the future for the targeted websites by cybercriminals with no moral political motivations. It would also allow morally- and security-considerate cyberdeviants to avoid high penalties for exploits that ultimately aim to improve security and protect citizen rights against state or corporate excesses or negligence. The adoption of such approaches would also remedy the problem of targeted companies resorting to courts for compensation for the offences, only to find that protesters' funds are inadequate or that the cases are unenforceable due to jurisdictional hurdles. The security advice and the eventual prevention of important breaches in the future would substitute for civil compensation. Of course, it should come as no surprise, , if protesters decline to assist in securing corporate or state networks due to their anti-establishment ideologies.[97] However, no single, particular solution can be totally successful and regulatory success will rely on the facilitation of the interplay of all the parts of the regulatory network and their potential contributions.

Potential cooperation between ethical hackers, law-enforcement and targeted websites owners would also be a step towards increasing the understanding of society and law-

[96] Thompson (n 53) 574.

[97] Mary M. Calkins, 'They Shoot Trojan Horses, Don't They-an Economic Analysis of Anti-Hacking Regulatory Models' (2000) 89 Georgia Law Journal 171*,* 205-6.

enforcement agencies of the beneficial aspects of moral hacking, which could gradually lead to less punitive and more understanding responses.[98] Moreover, as Thompson argues, avoiding the harsh punishment of ethical hacking would benefit moral hackers, without actually having an impact on the deterrence and treatment of purely criminal ones, as these safe harbour provisions would be inapplicable to those that act with criminal motives, cover their tracks and employ destructive tactics.[99] The need to engage more with ethical hackers for promoting cybersecurity has also been acknowledged in the UK Cybersecurity agenda, which suggests that cooperation of ethical hackers to assist with security should be one of the future regulatory goals.[100]

2.5 Technology-based penalties

The goals of efficient prevention and just deserts, which would, in turn increase the legitimacy of punitive decisions and reduce conflicts, could also be promoted by a systematisation of attribution of specialised Internet restrictions and community service penalties for convicted hacktivists. Specialised penalties would increase the acceptance of sanctions, since these would be considered more well thought out in accordance with the protesters' specific context, but also usually less harmful and socially beneficial than imprisonment and, therefore, consistent with the protesters' declared ultimate purpose, which is the promoting of community welfare. Penalties for cyberdeviants could range from a ban on Internet access to the monitoring of use after the imposition of restrictions or even the forfeiture of IT hardware and software.[101] Alternative penalties that substitute for incarceration, such as electronic monitoring, apart from appearing more lenient than prison, are also considered to entail a much lower cost for the society.[102] Community service penalties could also entail the provision of actual IT services to the community

[98] Michael Lee et al., 'Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal' (1999) 14 Berkeley Technology Law Journal 839, 872; Thompson (n 53) 575.

[99] Thompson (n 53) 578-9.

[100] Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London 2011) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf accessed 03 August 2013, 29.

[101] On the technologies and costs of such penalties see Ch 3, Part 2.2.4 The utility of incapacitating and reforming hacktivists.

[102] Adrian Furnham, Alastair McClelland, and Edward Drummond Baxter, 'The Allocation of a Scarce Correctional Resource: Deciding Who Is Eligible for an Electronic Monitoring Program' (2010) 40 Journal of Applied Social Psychology, 1606.

through teaching or covering IT needs of public services. In many cases the courts have found that for delinquency, which can exist only online, much like ECD, relating the penalty to the restrictions of use of the medium can be an effective and proportionate penalty.[103]

The penalties ought to be assessed in relation to nature of the offence, the technology involved and the potential of the sanctions for preventing recidivism.[104] Being more personalised and milder than incarceration penalties and actively socially beneficial through the potential provision of a community service, these penalties would better reflect the less censurable, moral and socially considerate intentions behind many hacktivist initiatives. These alternative penal choices also express a renewed focus on rehabilitation and not on sterile, punitive retribution and for these reasons they have been suggested by Supreme Court Judge Wollf in the US as a solution to the problem of increased punitiveness and have also formed part of official suggestions regarding the UK Cybersecurity Agenda.[105]

Penalties that relate to rehabilitation and code-based restrictions, rather than long imprisonment, satisfy the justifying reasons for punishment, from efficient prevention to just deserts. The enrichment and choice of case-specific penalties regarding each offender could potentially further produce a dialogue of the needs and desires of the offenders, the victims and society more generally, thus promoting a more symbiotic process between hacktivists, the legal system and the general society. In the UK, members of the Lulzsec group, which is an offshoot of Anonymous resorting to less morally motivated or political exploits, received punishments that for some entailed electronic tagging or community punishments.[106]

[103] Skibell (n 56) 944; Jessica Habib, 'Cyber Crime and Punishment: Filtering out Internet Felons' (2003) 14 Fordham Intellectual Property Media & Entertainment Law Journal 1051, 1054-5. See for example *US v Mitnick*, 145 F.3d 1342 (9th Cir. 1998); *US v Crandon*, 173 F.3d 124 (3rd Cir. 1999).

[104] Gabriel Gillett, 'A World without Internet: A New Framework for Analyzing a Supervised Release Condition That Restricts Computer and Internet Access' (2010) 79 Fordham Law Review 217, 220.

[105] Michael A. Wolff, 'Evidence-Based Judicial Discretion: Promoting Public Safety through State Sentencing Reform', (2008) 83 New York University Law Review 1389, 1416-7; Cabinet Office (n 100) 30.

[106] Davis was sentenced to 24 months in a young offenders' institute, of which he will serve 38 days as he has been wearing an electronic tag for 21 months that counts against his sentence time. Mustafa al-Bassam was sentenced to a custodial sentence of 20 months, with a two-year suspension and 300 hours of community work. For the other two offenders, one will serve 30 months (to serve only half) and the other 32 months. Susan Watts 'Former Lulzsec Hacker Jake Davis on His Motivations' (*BBC,* 16 May 2013) http://www.bbc.co.uk/news/technology-22526021 accessed 18 May 2013.

A concern is the balancing of the penalties in relation to the offenders' rights of access to technology and information. The increasing need of citizens to use digital technologies in order to participate in everyday economic and political functions generate questions as to the proportionality and predictability of harms flowing from such restrictions.[107] For example, an access ban on Twitter has been lifted for the 14 alleged members of Anonymous in the US, on the basis of restricting free speech, with monitoring of the medium being considered adequate to prevent reoffending.[108] The freedom to connect has been defined by US Secretary Clinton as 'the idea that governments should not prevent people from connecting to the [I]nternet, to websites, or to each other'.[109] The UN Human Rights Rapporteur has also found that total disconnection measures are disproportionate and has emphasised the need to preserve access, even during times of unrest.[110]

Given the importance attributed to connectivity, courts ought to consider the duration and broadness of the restrictions. For example, an absolute and permanent ban of access to Internet and digital technologies has been considered coercive and disproportionate.[111] In various cases, a complete ban on Internet access was not accepted by the court with the justification that it would prevent the offender from participating in everyday basic functions, from filing in tax reports to shopping online.[112] However, courts could moderate general bans through the introduction of temporal limitations.[113] Whether a general, yet temporary, limitation of use to Internet-accessing technologies could be justifiable for many ECD protesters, whose work and everyday social life could be closely related to the Internet is questionable. The decision for imposing such penalties, and their extent and duration, thus, ought to be the result of careful assessment for structuring the penalty

[107] Gillett (n 104) 227-8; Examples are *US v Sofsky*, 287 F.3d 122 (2nd Cir. 2002)(*Sofsky*); *US v White*, 244 F.3d 1199 (10th Cir. 2001)(*White*).

[108] The Smoking Gun, 'Judge Lifts Twitter Ban on "Anonymous" 14' (*The Smoking Gun*, 19 March 2012) <http://www.thesmokinggun.com/documents/judge-lifts-anonymous-twitter-ban-145792> accessed 30 August 2012.

[109] Dutton et al. 'Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet' (UNESCO, Oxford 2010) 7-8.

[110] Frank La Rue, '*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. VI. Conclusions and Recommendations'* (United Nations General Assembly*,* 16 May 2011) <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf> accessed 14 February 2013.

[111] Gillett (n 104) 246-7.

[112] See *White* (n 107) and also *US v Holm*, 326 F.3d 872 (7th Cir. 2003)*(Holm); US v Heckman,* 592 F.3d 400 (3rd Cir. 2010).

[113] Gillett (n 104) 246; See *US v Walser*, 275 F.3d 981 (10th Cir. 2001).

appropriately to the offender's personal and professional needs.[114] Another way prevention could be achieved without restricting access is through the choice of technology one is allowed to use. For a hacktivist, the restriction to use devices that have a predetermined degree of access to the Internet through some proprietary network and device could be an effectively preventive restriction on the employment of more controversial network applications, without unduly limiting access to basic services of the information society. As Zittrain has described,[115] 'tethered devices' such as iPhones or Microsoft xbox, operate on specific, privately managed networks, have specific, preset limits of access and do not allow much initiative to users in terms of downloading software or generating or modifying code. Consequently, users will still have access to the Internet and information online, but will be unable to download and use hacktivist tools and usage could be monitored and restricted more explicitly with the help of the service provider, but also the hardware's preset capabilities.

Having seen some options for potential changes to cybercriminal law and its enforcement, it is now time to discuss other preventive alternatives, where the role of technology and private actors will also be core elements.

3. From reaction to prevention

3.1 Collaborative symbiosis and concerns of legitimacy

As has been discussed at the beginning of this chapter, regulators should not just focus on reactive measures, such as resorting to courts, but ought to engage with additional actors and tools in also adopting preventive solutions. The acknowledged weaknesses of states to deal with cybercrime on their own, such as their lack of expertise and coordination, as well as the global enforcement of cybercriminal laws,[116] have initiated discussions for attributing

[114] The state should not impose technological use restrictions, if these would render the finding of work impossible. See *US v Russell,* 600 F.3d 631 (D.C. Cir. 2010) (stressing that McDonald's and PETCO require computer use to complete job application and duties, respectively); *Holm* (n 112).

[115] Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press, Virginia 2008).

[116] Ch 4, Part 1. Regulating hacktivism: The focus on 'command and control'.

a more active role to private actors in cybersecurity.[117] Technological controls might be able to remedy the indeterminacy of laws, the wording of which cannot always include all possible relevant incidents, especially when unpredictable technological effects are involved.[118] Preventive measures have been characterised as a useful alternative for avoiding the inefficient, costly and potentially stigmatising criminal process,[119] particularly since they can simultaneously efficiently reduce the losses by countering any impairing effects.

Governments have a keen interest in collaborating with private actors in order to promote more efficient and cost-effective policies in dealing with cyberdeviancy. Moreover, private actors also have an increased interest in pursuing preventive technological measures, because the prevention of disruption would result in reducing damages and loss from protests, in contrast to going through legal processes of civil compensation, which would require lengthy and costly procedures with doubtful benefits in relation to getting any compensation for the potential losses. Collaborative, preventive tactics would reduce hacktivism-induced dangers to cybersecurity before protesters could actually impact on the network and cause any serious disruption or acquire important information.

In relation to hacktivism, a realistic aim would not be the prevention of the protests or the existence of hacktivists per se, since hacktivism as an expression of dissent will always exist to a degree. The preventive efforts, thus, ought to focus mostly on reducing disruptions in general through the provision of more speech opportunities and the prevention of protests with potentially seriously harmful impact, such as attacks on critical infrastructures. The preventive efforts would be greatly enhanced through the engaging of digital technology and the support from private companies, since especially Internet conglomerates, such as Google or Facebook, for example, have more control over

[117] Aspen Institute, 'ASF 2011 Cyber-Security' (Aspen Security Forum Proceedings, *YouTube,* 29 July 2011) <https://www.youtube.com/watch?v=yoWkAVXmSs0> accessed 16 February 2013; Cabinet Office (n 100).

[118] Karen Yeung, 'Towards an Understanding of Regulation by Design' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008) 91-2.

[119] Jay P. Kesan and Ruperto Majuca, 'Optimal Hackback' (2010) 84 Chicago-Kent Law Review 831, 834.

technological resources online, as well as over the communicative platforms hacktivists employ for organising.[120]

The use of code tools and private actors in preventive functions online, though, entails serious implications for the legitimacy of these measures. The collaboration with the state in activities such as policing, the exercise of which has traditionally been considered to require political legitimisation, could put these private actors under the obligation to abide by the limitations and safeguards that state agencies have to abide by.[121] As Freeman argues, 'the exercise of regulatory power by private actors may undermine features of decision making that administrative law demands of public actors, such as openness, fairness, participation, consistency, rationality and impartiality'.[122]

As Black argues, assessments of the 'publicness' of the activities of private actors could be based on contextual, activity-based assessments, adopting a non-unitary, but flexible approach to defining 'publicness' and to imposing the related limitations, safeguards and reviewing processes to the particular actions of private actors that are deemed public.[123] Scott submits that courts have actually tended to review decisions that entail the exercise of public power, even if the organisations are private.[124] As he documents, the receipt of public funds by private bodies would, for example, render recipients publicly accountable through state audit mechanisms.[125] Moreover, it has been suggested that public law principles relate to private actors and that human rights could have a horizontal application for private actors that provide public services.[126] Consequently, especially for technological controls that might be implemented on a more general scale by private intermediaries,

[120] Social networking sites, such as Facebook, Twitter.

[121] For the debate of introducing private actors in policing and the problems this entails see Garland, *The Culture of Control: Crime and Social Order in Contemporary Society*; For policing through the employment of private actors and code and the problems with transparency and accountability see also Yeung (n 118) and TJ Mcintyre and Colin Scott, 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008); For policing as an original public good to be enjoyed by the whole public see Adam Crawford, 'Policing and Security as 'Club Goods': The New Enclosures' in Jennifer Wood and Benoit Dupont (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge 2006) 115.

[122] Freeman (n 1) 334-5.

[123] Julia Black, 'Constitutionalising Self-Regulation' (n 14) 52.

[124] Colin Scott, 'Accountability in the Regulatory State' (2000)27 Journal of Law and Society 38, 41.

[125] ibid.

[126] Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a" Post-Regulatory" World' (2001) 54 Current Legal Problems 103, 143-4.

such as traffic monitoring and blocking mechanisms, the democratic legitimisation should not just relate to a decision to adopt code-based, preventive measures. Instead it ought to extend to the practical implementation and administration of these projects in order to ensure that citizen interests are not compromised by the non-discretionary nature of technological controls or by means of implementation that are meant to serve private interests.[127]

The introduction of safeguards and reviewing mechanisms based on established notions of procedural justice could potentially be a step towards increasing the proportionality of responses as well as accountability, since, according to Koops, normative technologies that regulate behaviour should comply with criteria that society considers important for regulation.[128] Considering Baldwin's legitimacy criteria, which suggest a need to balance efficiency, fairness, accountability and legality,[129] it would appear that private actors will have to demonstrate, beyond efficiency and technical expertise, the ability to remedy the lack of formal, democratic legitimisation by demonstrating similar concerns for the rule of law and citizen rights. Criteria similar to those for promulgating laws, such as the constitutional substantive and procedural values, of liberty, legal authorisation, transparency, proportionality and individual choice, should therefore be at the forefront of legitimacy assessments for state and private preventive technological schemes.[130] How such elements could be integrated in preventive regulatory measures will be discussed through some more specific suggestions for preventive measures that could supplement the efforts to regulate hacktivism.

3.2 Three modes of preventive symbiosis

3.2.1 Creating spaces and processes of dialogue

[127] Yeung (n 118) 97; McIntyre and Scott (121) 118-21.

[128] Bert-Jaap Koops, 'Criteria for Normative Technology: The Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008).

[129] Baldwin (n 6).

[130] Lessig, *Code v.2.0* (n 32); Joel R. Reidenberg, 'States and Internet Enforcement' (2004) 1 University of Ottawa Law & Technology Journal 216; See also Jay P. Kesan and Shah C. Rajiv, 'Deconstructing Code' (2003-4) 6 Yale Journal of Law & Technology 277, <http://ssrn.com/abstract=597543> accessed 13 June 2008; Koops (n 128) 162-4.

The illegal nature of hacktivism partly reflects the speech deficit that privately controlled spaces online create, as discussed previously.[131] Therefore, the need to resort to hacktivist disruptions could be reduced through the provision of additional deliberative processes and spaces. These could allow for more expressive freedom and also facilitate inclusive and equal dialogic conditions between speakers, rather than preserve the dominant relations of power that the current media scene attributes to power factions, such as governments and private online companies and media conglomerates.[132] Consequently, efforts should not just focus on bringing diverse regulators together, but on the conditions that this dialogue is being realised. The dialogic process would benefit from open and critical fora that could allow reconsideration of the participants' views without power inequalities steering discussions and decision-making.[133]

In order to facilitate the dialogic assessments and decision-making in ways that also respect already established processes, regulators ought to reconsider multi-stakeholder processes, as the first level to decentralising regulation and power.[134] Improvement could begin by assessing the institutional background within the context of which the dialogue takes place, the efficiency of the processes as they are structured in relation to achieving the goals of decentralised, equal and accountable deliberation and the problems the current methods might create in relation to the special characteristics of the expected participants.[135] For example, conditions giving priority to state actors compared to civil society, either in terms of how the forum is institutionally constructed to prioritise states or to whether the processes are resource-demanding, thus, excluding financially weaker parties, could inform some initial considerations for restructuring deliberative fora. This reassessment could be useful for all regulators (states, corporations and civil society), especially since the current realisation of multistakeholderism, such as the Internet

[131] Ch 2, Part 1. Free expression and hacktivism.

[132] Manuel Castells, *Communication Power* (Oxford University Press**,** Oxford 2009) 72-4.

[133] Morgan and Yeung (n 28) 36-7.

[134] See Ch 1, Part 1.1 Defining regulation and 1.2 The modern networks.

[135] Similar characteristics are the focus of regulatory assessments in responsive models of regulation articulated by Black and Baldwin, trying to demonstrate the need for a more holistic understanding of the context and the effects of regulatory solutions. Robert Baldwin and Julia Black, 'Really Responsive Regulation' (2008) 71 The Modern Law Review 59.

Governance Forum (IGF), has been criticised as failing to promote equality, diversity and global representation.[136]

As Lovink and Rossiter emphasise:

> [T]he people benefiting from such endeavours as the World Summit of the Information Society are, for the most part, those on the speaking and funding circuits, not people who are supposedly represented in such a process. Networks call for a new logics of politics, one based not just on a handpicked collection of NGOs that have identified themselves as 'global civil society'.[137]

Considering the problem of formalism in the official fora, such as the IGF, where talks take place under the UN auspices and are recorded,[138] multi-stakeholder models could gradually be structured in less formal ways and with more direct, interactive deliberative processes and engaging more with digital technologies in order to allow groups from around the globe to voice their views and suggestions. Generalising distance-participation would facilitate more accessible, inclusive and accountable decisions and consequently, more democratically legitimised decisions on Internet issues, which could help reduce conflicts and protests. Informal deliberative processes enable more substantive and inclusive discussion for a wider spectrum of civil society actors, especially since hacktivist collectives, as a more informal part of civil society, would avoid formal organisational models.[139] The informal interaction structures, which could be characterised as 'everyday multi-stakeholderism', should thus facilitate a more dynamic and constant interaction between actors, on a more frequent and informal basis that will establish an ongoing flow of information and opinion-exchange mechanisms between regulators.[140]

[136] Arne Hintz, 'Deconstructing Multi-Stakeholderism: The Discourses and Realities of Global Governance at the World Summit on the Information Society (WSIS)' (Central European University, Budapest 2007) 3-4; Rebecca Mackinnon, *Consent of the Networked:The Worldwide Struggle for Internet Freedom* (Basic Books, New York 2012) 208.

[137] Geert Lovink and Ned Rossiter, 'Dawn of the Organised Networks' (2005) 5 Fibreculture Journal <http://five.fibreculturejournal.org/fcj-029-dawn-of-the-organised-networks/> accessed 15 February 2013.

[138] Dmitry Epstein, 'The Duality of Information Policy Debates: The Case of the Internet Governance Forum' (DPhil, Cornell University 2012)http://core.kmi.open.ac.uk/display/6103666 accessed 13 June 2013, 115-6.

[139] Arne Hintz and Stefania Milan, 'At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy' (2009) 5 International Journal of Media & Cultural Politics 23*,* 34.

[140] ibid.

It has been argued that in order to proceed with attempts to create functional dialogic fora, there would have to be a consensual normative base, where some basic presumptions in relation to governance will inform the further policy discussions.[141] But how could we achieve normative consensus in an environment where actors with different normative backgrounds and interests interact within these processes? We would potentially need to adopt a pre-procedural agreement that no norms would be imposed. As Castells argues, a common culture and understanding between the networked societies today does not rely on homogenising social values, but on sharing the value of communication. This can allow different groups with diverse cultural backgrounds and interests to come closer, not through agreeing on the content of the communication, which could exclude dissent, but primarily on the processes of communication, allowing diversity and dissent to play a co-evolutionary role in more legal and efficient ways and processes than network disruptions.[142] Ladeur has argued that in order to reinvent proceduralised legal discourse,[143] for example, we should not focus on common principles, such as achieving consensus and veracity, especially at a global scale, but should instead seek to promote secondary virtues, such as keeping a variety of options open and tolerating multiple opinions and allowing the use of language games for everyone, which would eliminate self-reinforcing discourses.[144] Since the use of language games according to Wittgenstein expresses a specific way of life and particular actions into which the specific use of language is woven,[145] allowing the shared use of language games within the multistakeholder processes would, absolve the discussion from reinforcing the rationales and actions of only the side the language games of which are generally employed. Bringing the discussion on an equal ground even on a linguistic level, would thus also reduce the hacktivist need to resort to disruptive interventions of dominant symbols, which are responses to a monopolisation of dominant

[141] Milton Mueller, John Mathiason and Hans Klein 'The Internet and Global Governance Principles and Norms for a New Regime' (2007) 13 Global Governance 237.

[142] Castells (n 132) 39.

[143] As Black explains: 'proceduralisation is a term which is used to encompass both the basket of new techniques of regulation which characterize or are prescribed for the 'post' regulatory state including enhanced participation, and the quite particular technique, advocated by Teubner, of changing organisational processes so as to ensure internal democratization and external responsiveness.' Black, 'Proceduralisation and Polycentric Regulation' (n 41) 99.

[144] Karl-Heinz Ladeur, 'Prozedurale Rationalitaet – Steigerung der Legitimationsfaehigkeit oder der Leistungfaehigkeit des Rechtssystems?' 7 Zeitschrift fuer Rechtssoziologie, 265*,* 273 cited in Teubner, *Law as an Autopoietic System* (n 17) 68.

[145] See Ludwig Wittgenstein, *Philosophical Investigations* (G.E.M. Anscombe tr, 2nd ed Blackwell, Oxford 1958).

discourses by specific factions. The facilitation of these elements should thus inform the ways dialogic processes ought to be structured.

The realisation of this overarching norm of communication today could also help regulators reconsider representational, deliberative models in the structuring of everyday multi-stakeholderism, which would make these processes more inclusive and efficient through processes that also correspond to modern grassroots political organising.[146] The introduction of new norms and processes could be further facilitated by engaging more with the technical/hacker community in general, which is often more informed, specialised and has realistic practical perceptions about the needs and possible regulatory solutions applied to Internet-related problems. Even through its formalised processes, deliberative fora, such as the IGF, are gradually transfusing values of the online communities such as freedom of information into the Internet governance processes.[147] The multiplication of the sources and processes through which citizen values can be transfused into policy-making discussions will also eventually increase the legitimacy of the policies decided, allowing the wider civil society to take part in the construction of broader political decisions,[148] thus reducing conflict and the need for more forceful expression through symbolic, disruptive protest. Even if hacktivist groups do not join such processes, hacktivists are often also part of other political collectives that could be included in the new more creative, informal processes, thus reducing the need to resort to illegal disruptions.

Irrespective of efforts to increase deliberative opportunities, hacktivist actions would not be eliminated, since the problems they relate to are so numerous and the conditions of speech inequalities so pervasive that there will often be potential justifying reasons for CD protests offline and online. However, that does not mean that we should not attempt to reduce disruptive protests in a creative manner that addresses the deeper causes of the disruptions. Consequently, the proliferation of more deliberative and inclusive fora should not be seen as the co-opting of hacktivism by groups, tactics and purposes that are more traditional. Instead it should be seen as an attempt to open up deliberation in acknowledgment of what hacktivism represents and demands, and to reduce the speech deficits that generate the need for more hacktivist protests.

[146] Ladeur (n 144).
[147] Epstein (n 138).
[148] Castells (n 132) 12.

3.2.2 Online intermediaries and contractual terms

Another way for service and content providers such as Verizon, Facebook or YouTube to regulate the activities of hacktivist groups is through the use of terms of service. These companies impact on hacktivists' organisation, functionality and communication through the use of contract terms and business policies for allowing the use of their online communications platforms, the provision of access or hosting services and even the processing of financial contributions. Private actors could, either in relation to their own policy desires or after a related implicit or explicit state, demand to impose restrictions on hacktivist groups in order to influence their organising and communication.[149]

In order for these contract-based, corporate regulatory policies to preserve their legitimacy, they would need to preserve proportionate and accountable treatmentfiltering of controversial speech and groups. This could be done by establishing opportunities for second-level review by users against decisions that, without any provided justification, violate their rights of privacy, speech and access. On that basis, processes of resolution that promote the interaction between the alleged publisher of illegal content, requesting it to be taken-down will be a very positive step. In the US for example, the Digital Millenium Copyright Act (DMCA) includes a provision that relates to countering notices for take-down of materials that are considered to infringe copyright.[150] The rationale behind the counter-notice is to assess whether the complainant that requested that certain content be removed has indeed a legitimate interest in this act and is willing to pursue it in courts, rather than just acting in bad faith.[151] Counter-notices have not been employed extensively, as most people are ignorant of the existence of such a provision.[152] However, this provision could constitute a guiding example of how the appeal processes for arbitrary decisions to remove content on behalf of content providers could be countered. Allowing users to appeal take-down decisions through quick arbitration processes provided by the website administrators would produce more legitimate processes by providing a more transparent and validated process for service and content providers to eventually proceed with the

[149] See Ch 4, Part 4. The role of private actors.

[150] 17 U.S.C. Section 512 (g)(3).

[151] See Sections 512(g)(2)(B) and 512(g)(2)(C). See also Lydia P. Loren, 'Deterring Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously' (2011) 46 Wake Forest Law Review 745, 757-8.

[152] ibid.

filtering requests.[153] These changes will impact not only on hacktivists, but also generally on citizens' expression and interaction online. However, since hacktivists often act controversially and interact with the authorities, the regulatory benefits will be even more obvious in these cases.

Service providers could deter protesters from resorting to excessively harmful or immoral protests[154] by declaring a willingness to decline services to groups that repeatedly resort to immoral or seriously harmful cyberprotests or controversial speech.[155] However, decisions to decline a service, in order not to induce further protest, should be based on clear and transparent terms and conditions. Moreover, quick arbitration processes by regulatory bodies ought to exist in order to protect consumers from contractual interpretations that excessively compromise the rights of users and businesses to access funds or advertise their products and views, since particularly the blocking of funds could seriously compromise the viability of non-profit, civil society organisations. Unsubstantiated denials of service by companies could also be brought to court as breaches of contract, especially in cases where the declined service is crucial for the operating of the client. The freezing of funding for Wikileaks by Paypal and Visa is again a characteristic example of arbitrary and unjustified denial to provide a service that is solely based on political choices to stifle speech, even though there have not been any charges filed against the whistleblower website. Considering that it took more than a year in order for the case of WIkileaks against Visa to be decided in favour of Wikileaks, it would appear that speedier arbitration processes should be installed to prevent companies that offer such crucial services from behaving so arbitrarily, potentially in the form of arbitration in dispute resolution processes. The more important these organisations become for online expression and its financial support, and the reaching of wider audiences, the more their actions ought to be checked, as if they were performing a public function.[156]

However, adoption of stricter safeguards is contradictory to their profit-making purposes and their need-to minimise risk-related activities, such as interacting with

[153] Benoit Frydman and Isabelle Rorive, 'Regulating Internet Content through Intermediaries in Europe and the USA' (2002) 23 Zeitschrift für Rechtssoziologie 41, 52 analyses the US approach, which adopts such interactive processes.
[154] See Ch 1, Part 3. The criteria of justifiability.
[155] Stacey D. Schesser, 'A New Domain for Public Speech: Opening Public Spaces Online' (2006) 94 California Law Review 1791, 1800.
[156] Part 3.1 Collaborative symbiosis and concerns of legitimacy.

controversial political groups. Consequently, the more these private actors become established, the more they will want to avoid being associated with hacktivists. However, there is also the opposite side that links the survival of businesses online to demonstrating a commitment towards the promoting of justice for customers and society. In general, such a stance usually increases social trust, which consequently reduces protests that could threaten the businesses' social acceptability, functionality and profits, and even advertises these companies as user-friendly, rather than as private police.[157] Therefore, the preservation of substantive rights and procedural safeguards for moral protesters could eventually prove more beneficial for these companies than indiscriminately collaborating with the authorities or acting as private police, as it could lead consumers to embrace such companies and protect it from expressions of disaffection that would be translated in the form of hacktivist disruptions.

3.2.3 Technological defences and countermeasures

A third example relates to monitoring and filtering of IP-addresses and blocking websites that are advocating hacktivist actions that, for example, target sensitive targets or promote damage rather than expression as a dominant goal. Identifying the various types of traffic in order to prevent DoS-related traffic to a target, for example, could be facilitated for targeted websites and ISPs through their collaboration with other cybersecurity companies and initiatives.[158] Preventive code-based solutions, such as blocking or filtering, which could potentially require some form of traffic monitoring and management, could impact on the ways traffic is generally managed in cyberspace, according to its nature and origin thus potentially compromising net neutrality.[159] Net neutrality has been considered a core principle for the Internet, both in the US and the EU. The US Congressional Research Service argued that: '...owners of the networks that compose and provide access to the Internet should not control how consumers lawfully use that network; and should not be able to

[157] Christine Parker, *Just Lawyers: Regulation and Access to Justice* (Oxford University Press, Oxford 1999) cited in Braithwaite (n 26) 262-3.

[158] CISCO, for example, compiles lists of domain names and IP addresses related to malign web-traffic and spamming email servers, facilitating filtering of malign traffic. CISCO, 'Combating Botnets Using the CISCO Asa Botnet Traffic Filter' (*CISCO White Paper,* 2009) <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/white_paper_c11-532091.html> accessed 26 February 2012.

[159] Net neutrality has been a major aspect of the original Internet. See Ch 1, Part 1.4 The shifting power balance in cyberspace.

discriminate against content provider access to that network'.[160] The EU has set out its views on net neutrality in art 8(4)(g) of the Framework Directive stating that: 'The National Regulatory Agencies shall promote the interests of the citizens of the [EU] by:[...] (g) promoting the ability of end-users to access and distribute information or run applications and services of their choice'[161]

However, defending against attacks considered detrimental to the network could not be subordinated to the net neutrality principle as its inviolability has been challenged by states and corporations on grounds of security. As the Federal Communication Commission (FCC) chairman said:

> [T]he Commission's network principles only recognize and protect user's access to legal content. The sharing of illegal content, such as child pornography or content that does not have the appropriate copyright, is not protected by our principles. Similarly, applications that are intended to harm the network are not protected.[162]

In the UK, the House of Lords Select Committee on Science and Technology argued that the changes in technology and the needs and ways for the provision of security require more holistic approaches, engaging private security market actors and also reconsidering adherence to net neutrality.[163] Traffic inspection and management could also have privacy implications for users, violating data protection legislation,[164] although as the EU data protection supervisor has argued, network security has always been a reason for

[160] Angele A. Gilroy 'CRS Report for Congress: Net Neutrality: Background and Issues' (Congress Research Service, 2008) <http://www.fas.org/sgp/crs/misc/RS22444.pdf> accessed 13 June 2013.

[161] Council Directive (EC) 2002/21 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L 108; See discussion on the benefits and problems arising from discarding net neutrality in Wu and Yoo, 'Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate' (2007) 59 Federal Communications Law Journal 575

[162] David Kravets, 'Analysis: FCC Comcast Order is Open Invitation to Internet Filtering' (*ThreatLevel Blog,* 20 August 2012) <http://www.wired.com/threatlevel/2008/08/analysis-fcc-co/> accessed 23 June 2013.

[163] House of Lords Select Committee on Science and Technology, 'Science and Technology - Fifth Report' (London, 2007) <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm> accessed 20 May 2013.

[164] The legal framework is mainly Art. 5(1) of the Council Directive (EC) 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)(ePrivacy Directive) OJ L 201 requires that users involved in communications must give their consent for the monitoring of communications and traffic data to become legitimate.

monitoring and discriminating traffic.[165] Apart from specific groups engaging with IP-tracing and listing that enables filtering of undesired traffic based on its origin, eventually there will be a general need for telecommunications service providers to employ harmonised and standardised trace-back tools and subsequently even IP-listing, as part of a general forensic tracing obligation that private actors will need to satisfy in collaboration with the authorities for crime prevention purposes.[166] In addition, as seen in chapter four,[167] in the US the National Security Agency (NSA) has been found to have access to random communications of subscribers of major ISPs and content providers.[168]

Faced with the risks for arbitrariness and lack of transparency regarding private actors' capability to monitor and block traffic, especially under security premises, the creation of safeguards for assessing the need and the extent of this monitoring appears to be a crucial step towards preserving legitimacy by balancing such practices against citizen privacy and expression. However, assessments regarding security should thus also employ traffic management measures after their proportionality has been assessed against the potential threat. In the cases of virtual sit-ins, for example, a gradual evaluation of the potential disruptiveness of the traffic generated might be a more appropriate approach compared to pre-emptively blocking a hacktivist website discussing a political issue or blocking traffic by IP addresses that have been connected with hacktivist activity. Service providers could opt to monitor irregular activity not in terms of content, but in terms of origin, quantity and targets and try to reduce what might appear to be threatening mass traffic towards specific infrastructural websites and networks.[169]

[165] Restrictions on violating net neutrality can be bypassed when the operations relate to increasing networks security and detecting harmful activities in addition to network management, such as interconnection and billing. European Data Protection Supervisor 'Opinion of the European Data Protection Supervisor: On Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data' (Brussels 2007) <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf> accessed 13 May 2013> 4.

[166] Malcom Shore, Yi Du, and Sherali Zeadally, 'A Public-Private Partnership Model for National Cybersecurity' (2011) 3 Policy & Internet 1*,* 18.

[167] See Ch 4, text to (n 274).

[168] Stephen Braun et al. 'Secret to Prism Program: Even Bigger Data Seizure' (*Associated Press*, 15 June 2013) <http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure> accessed 21 June 2013.

[169] Shore, Du and Zeadally (n 166) 16.

Reducing arbitrariness in these filtering processes could be further facilitated by targeting addresses that have been blacklisted by other companies.[170] Such a targeted way of defence could help defend against traffic from botnets during virtual sit-ins, allowing protesters to make their stand without overtly high disruptions to the defending websites. However, blacklisting criteria ought to be subject to review as well, and these criteria should also be based on codes of practice that public regulatory bodies, in conjunction with private listing companies would establish to guarantee common standards, transparent procedures and appeals processes. Reviewing processes and procedural safeguards will have to be identified and applied in order to decide on the disproportionate or undue use of monitoring traffic or filtering potentially by instituting assessment and appeal processes for users at the level of regulatory bodies or even in courts.

Justifying the employment of controversial technological interventions against hacktivist protests would, thus, also need criteria of potential dangerousness in relation to the nature of the target and the services it provides. Regulators, for example, could accept or even advocate monitoring and blocking when potentially disruptive traffic is being directed towards sites and services that relate to critical infrastructures, such as power grids or banking websites. The designation of critical infrastructure is a crucial stage of this process, since the combination of such a decision with the ever-expanding list of what is considered a critical infrastructure online[171] could lead to a generalised monitoring duty for ISPs.[172] This duty could, in turn, have serious implications for Internet traffic, ISPs' financial viability, accessibility of controversial Internet content and user privacy. In order to avoid the risk of imposing extensive monitoring regarding an array of critical infrastructure websites, assessments of the critical nature of specific websites ought to be based on the actual

[170] CISCO (n 158).

[171] The US Department of Homeland Security has defined as critical IT sector functions: IT products and services; Incident management capabilities; Domain name resolution services; Identity management and associated trust support services, Internet-based content, information, and communications services Internet routing; access, and connection services. Department of Homeland Security, 'National Infrastructure Protection Plan: Information Technology Sector' (undated) <http://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-information-technology-snapshot-2011.pdf> accessed 30 August 2012.

[172] For example, art.4 of the ePrivacy Directive (n 164) obliges ISPs to take appropriate measures for safeguarding network security, thus, legitimising inspection techniques that aim to filter dangerous traffic, such as viruses, yet always within the limits of proportionality. European Data Protection Supervisor (n 165) 11.

function they serve and not its institutional categorisation.[173] Categorisation of critical infrastructure websites would assist in generating manageable differentiations and categorisations of critical and non-critical targets online and would create more transparent processes in justifying the decisions to employ technological preventive and monitoring tools against attacks on these networks. Finally, it would also assist hacktivists in avoiding the targeting and compromising of infrastructural systems in the first place.

The employment of technological measures could also take a more aggressive form - actually causing some form of counter-disruption to the attacking computer systems - which generates further legitimacy concerns, even though such countermeasures had been employed by the US government against an EDT protest in the past without much concern for the consequences.[174] However, the nature and gravity of technology and networks has increased exponentially since then and actors employing counterattacking tools would have to take into account moral and practical challenges, since counter-attacks could cause undue damage to innocent users and induce retaliation from protesters. The main concerns flowing from the employment of counterattacking software are maintaining the proportionality of harms between the protest and the counterattack, the potential side-effects of the counterattacks and the accountability of the counter-attackers. Accountability concerns are even more pertinent due to the potential for disruption of compromised computers engaged in the protests, as they might belong to providers of critical services, for example, a hospital computer used by protesting hackers after having become part of a botnet.[175] Even if state agencies or private companies do not care about compromising the functionality of individual user-protesters, the risk of indiscriminate counterattacking, which could result in compromising a critical computer system, ought to be an adequately serious concern that would induce a more considerate deployment of aggressive technological countermeasures.

[173] The webpages protected would have to provide crucial information or the nature of the website should reflect a strong reliance for viability of the organisation it represents on its accessibility.

[174] Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Jon Arquila and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND Corporation 2001) 265.

[175] Curtis Karnow, 'Launch on Warning: Aggressive Defense of Computer Systems' (2004) 7 Yale Journal of Law & Technology 87, 93; Counterstrike-software companies do not exclude the chance of small, collateral damage to innocent parties. Although it is suggested that if the exact address of the attacker cannot be verified as not being of such critical nature, less aggressive measures should be preferred, expressing the need to minimise risk. Bruce P. Smith, 'Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help' (2005) 1 Journal of Law Economy & Policy 171, 181.

Criteria for assessing proportionality and preserving legitimacy during the use of countermeasures could be drawn from traditional legal processes that justify actions relating to necessary preventive acts against an imminent harm and shouldering liability for potential excesses.[176] Reidenberg, for example, argues for the need to prescribe strict authorisation criteria that are consistent with democratic societies' rule of law values.[177] In these cases of attack and counterattack, proportionality is the first principle that comes to mind. Aggressive countermeasures ought to be employed, for example, after assessing the origin of the targeted computers or, at least, by moderating the designated disruptions to the computer systems counterattacked, thus minimising the risks of undue harms to critical resource computers. For example, a hackback that is aimed to destroy the hard-drives of protesters participating in a short-term virtual sit-in would not be justifiable as disproportionate to the harm of the original attack. Brenner, in justifying counterattacks, also employs the right to defend ones' property, if the defender can prove that there was no alternative means of protection in a timely manner that would entail less force than a code-based counter-strike.[178] Justification will, of course, rely on assessments regarding the nature, imminence and potential disruptiveness of the attack. For private actors, accountability could also be assessed on the basis of self-defence, which could legitimise the private use of reasonable force, even if force and counterforce in hacktivism are expressed in technological form, such as through denial of service attacks.[179] In cases that counterattacking organisations mistakenly or excessively employ potentially damaging counterattacking measures that exceed the limits of a reasonable mistake, they would also be liable in court for failing to abide by proportionality standards and could compensate those harmed from unjustifiably disproportionate counterattacks.[180]

The moderation of the effects caused by the countering tools should also be proportionate in order to prevent escalation of counterattacks. Avoiding protester retaliation would be facilitated if the counterattacks demonstrate the intention of those employing those tools to act preventively and protectively, rather than retributively and

[176] See Part 3.1 Collaborative symbiosis and concerns of legitimacy.

[177] Joel R. Reidenberg, 'Technology and Internet Jurisdiction' (2004) 153 University of Pennsylvania Law Review 1951, 1964.

[178] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger Publishers, Oxford 2010) 212-4.

[179] Kesan and Majuca (n 119) 832-3.

[180] Reidenberg, 'Technology and Internet Jurisdiction' (n 177) 1965; Consideration of proportionality and accountability have also been based on the defences of choice of evils or necessity. Smith (n 175) 191-2.

excessively. This would mean that, even if a counterattack is employed, a legitimate aim would be to stop the initial protesting attack and not to destroy the protesters' computer resources. After all, protests, such as virtual sit-ins, are based on the use of elementary tools for targeting websites with information requests (LOIC) or non-harmful viruses, which could not be employed in an escalating way and are not by themselves damaging tools, apart from when masses of people join the protests. Consequently, countermeasures ought to reflect the threat that technological tools of hacktivists pose. Although the disruption of the protests might be reduced through preventive or counterattacking tools, the purpose of hacktivists will not be totally nullified since the success of these protests relates also to the receipt of public disaffection by the defending target, as well as to the initial organising of protesters towards a common goal rather than just on the degree of the final disruption.[181]

Apart from a perpetrator of counterhacks itself, the state, could take a supervisory role. This would not just involve the judicial system, which could resolve any conflicts relating to excessively damaging counterattacks, but would also involve promoting moderation by generating legislation or, at least self-regulation. Self-regulation policies or codes of practice would mandate limitations and standards for the use of tools that could have a harmful impact on user computers, as well an obligation to take any required measures to avoid adversely impacting on potentially compromised computers that might be providing important social services. The attribution of specific IP addresses to infrastructural systems and the compilation of lists of these addresses for use by those services and companies allowed to employ counterattacking tools could also facilitate more secure counterattacks.

4. The role of hacktivists

4.1 The role of hacktivists and users in the process of their regulation

The hacktivist community has an important role to play in the promotion of more appropriate regulatory solutions, since the behaviour and choices of the hacktivist community influence the way hacktivists themselves are perceived and treated by other

[181] See Ch 2, Part
3.3 Efficiency and the conflict of speech rights.

regulatory actors.[182] As discussed throughout the thesis, the radicalisation of the protests, with the inevitable disregard of moral safeguards, such as openness or non-harmfulness, has further justified crack-downs by the authorities on hacktivists in general and also, more specifically the acceleration of security processes with the excuse of the 'hacktivist threat'. Moreover, the current extreme hacktions, mainly under the banner of Anonymous, have served to delegitimise protesters by obscuring the symbolic protest role of hacktivism, thus making hacktivists appear retaliatory and leading in turn to further marginalisation.[183] In order to avoid all these problematic consequences, a return to the greater self-regulation of the first era of hacktivism appears to be a highly sensible route; although the rise in prosecutions[184] can also be attributed to the gradual intensification of legal restrictions. Although the intensification of restrictions online means that prosecutions will be more forthcoming in any case, the maintenance of moral standards that hacktivists initially adopted will give protesters a better chance to justify their actions in court and perhaps gain public support and sensitise prosecutors, judges and the jury in particular, while reducing overall cybersecurity concerns for their actions. One cannot expect or hope for a reduction of radical approaches from the state without the parallel demonstration of more socially-considerate behaviours by the protesters.

Self-regulation is 'the situation of a group of persons or bodies, acting together, performing a regulatory function in respect of themselves and others who accept their authority'.[185] Hacktivist communities often demonstrate a mix of 'voluntary self-regulation', where there is no link to a governmental influence, with more coerced behaviours, which are, for example, responses to the potential threat of prosecution by the state.[186] The stricter the regulation by the state, the more that voluntary self-regulation subsides, giving way to coerced self-regulation.[187] However, coerced behaviours are less guaranteed to survive, especially where the behaviour in question is already a reaction to a socially

[182] See Part 1.2 Balancing multi-actor regulation and the need for symbiosis.

[183] Anonymous have gone beyond symbolic protests by hacking into corporate and police networks and exposing credit card information or personal addresses of policemen involved in protest arrests that have been considered purely retaliatory, with low politically expressive quality. See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism.

[184] Actions of EDT and the Electrohippies or even the Lufthansa protest in Germany, where protesters were acquitted, are examples of group that, even though operating openly, did not have to face prosecution in the earlier years.

[185] Black, 'Constitutionalising Self-Regulation' (n 14) 26-7.

[186] ibid.

[187] See Ch 3, Part.2.2.3 Are highly punitive sanctions for ECD utilitarian?.

coercive phenomenon and can, thus, easily turn to radicalisation and disobedience of even community self-regulation norms as inefficacious. For example, openness about the identity of hacktivists was an initial voluntary choice of the protesters. However, the high penalty risks that current legislation can entail for those protesting openly have weakened the insistence on openness and various Anonymous have been discussing anonymity-enhancing tactics.[188]

State governance would be impossible if the systems and subsystems regulated do not also have the willingness and the organisational capacity to moderate their behaviours and force compliance through mechanisms within the systems.[189] Consequently, the self-regulation of hacktivist communities is crucial, even though the process presents interesting challenges regarding the regulability of current forms of political collectives online. Hacktivist collectives are an active node in the regulatory process and have demonstrated a measure of self-management in terms of promulgating basic rules of behaviour, guidelines for use of their tools and democratic decision-making processes through user fora.[190] Preserving and intensifying self-regulation of these communities would be a very important step in the process of generating moral legitimacy. However, self-regulation is also crucial for supporting approaches which are more balanced than the current ones adopted by the other regulators, such as governments or private companies, since protester self-regulation would facilitate the reduction of disruptiveness and would thus require more lenient controls. As has been discussed throughout the thesis, the preservation of certain moral criteria, such as openness, non-harmfulness or the existence of a justifiable political motive, is very important for supporting the distinction between hacktivist protests and plain cybercrime and, consequently, the need to facilitate regulatory conditions that can respond to these restrictions.

However, there are two challenges regarding the self-regulation of hacktivist communities. The first is the nature of these collectives, which are more amorphous than traditional communities and, therefore, often appear to lack the authority for designating

[188] Anonymous 'AnonNews - Everything Anonymous' (*AnonNews,* 08 March 2011) <http://anonnews.org/?p=comments&c=ext&i=996> accessed 21 June 2013.

[189] Black, 'Decentring Reguation' (n 126) 125-6.

[190] See for example the guidelines by the Electrohippies regarding their actions and the use of their virtual sit-in tools, or the user-license created by Hacktivismo regarding the use of their tools for non-criminal purposes in Ch 1, Part 2.2.1 The first era of hacktivism and the birth of electronic civil disobedience.

and imposing moral standards. The second is that, they have no concrete membership. Therefore, any sanctions for violation of norms could be hard to impose efficiently, either for lack of any impact on members, who might not have formal relations with the collective or due to the difficulty of locating the perpetrators. Let us then discuss how these challenges impact on the setting of normative standards and the imposition of the above sanctions.

4.2 The lack of authority and consensual moral/tactical standards

The first step towards proper regulation is a common effort by the protesters to articulate and preserve the moral and tactical characteristics that support the legitimacy of hacktivist actions, particularly by increasing fairness, proportionality and accountability. This effort will allow for the preservation of the moral character of hacktivist practices and will also set the criteria for imposing community sanctions when communal norms are disregarded. This first stage is crucial because, without the preservation of prescribed moral guidelines by the protester community, the activities could more easily deteriorate into plain criminality. The effort of hacktivist communities to facilitate the organisation of moral activities, and to avoid serious compromises of online security and, subsequently, the negative 'labelling' of the movement, could begin from promulgating and publicising specific moral standards.[191]

Another important aspect for demonstrating and preserving the moral character of hacktivist practices is the use of rhetoric that does not alienate citizens and other regulatory parties through its radical or vigilantist character, as often occurs with Anonymous,[192] but ideologically supports any designated moral standards and justifies the hacktivists actions politically. As Meikle argues:

[191] Earlier groups have been more eloquent in suggesting safeguards. In groups with an organising core, such as EDT, the realisation of the various protests entailed specific tactical guidelines in order for the actions to be as harmless as possible and demonstrate their moral motives: ibid. Even with less structured collectives like Anonymous, similar guidelines have been often deliberated and even publicised with online videos for online and offline protests: Anonymous, 'Anonymous - Code of Conduct' (*YouTube,* 21 December 2010)<https://www.youtube.com/watch?v=-063clxiB8I> accessed 16 February 2013; Anonymous, 'Protest in the Digital Era: DDoS and the Online Sit-In' (*Truthisrevolutionary*, 16 December 2010) <http://truthisrevolutionary.org/news/protest-digital-era-ddos-and-online-sit> 20 May 2011.

[192] See Ch 1, Part 2.2.2 Anonymous and the second era of hacktivism.

> [P]romoting an emergent cyberspatial politics as 'hacktivism' means dealing with the baggage of the 'hack' component of the term. This term may make it all too easy for electronic civil disobedience to be marginalized and demonized in turn. One challenge for activists, then, is not just to formulate new strategies and tactics appropriate to a shifting mediascape, but to recognize the ongoing need to create a careful vocabulary for discussing those tactics and strategies.[193]

In order to facilitate more patience and understanding between hacktivists and the other regulating factions, protesters ought to make efforts to develop a more responsible political language and argumentation that could be less easily portrayed as irresponsible, retaliatory and, consequently, politically illegitimate. The concreteness of the posed political arguments could increase the political acceptability and the legitimacy of protesters, and could induce more open dialogue between regulating actors, potentially forcing them to respond in a more dialogic and less conflicting way, thus promoting high quality deliberation. Although the different style and use of language are inevitable and pervasive in the current political systems,[194] the use of different styles should aim at producing dialogue, rather than expressing condemnation and sterile retaliatory tendencies that would induce a further defensive or condemning response from the other actors in the network. As Gardiner argues, even for proponents of more dramatised and alternative ways of using ironic or paradoxical language and symbolisms as a politically contestational tool, not unlike hacktivist culture jamming language,[195] reaching some sort of agreement in dialogue must be seen as an important goal.[196] Therefore, even if the protesters' hacktions manage to subvert the language of their targets during the event, the language employed before and after the event is also important in making actual political use of these expressive hacks,[197] integrating hacktivist performances into concrete political arguments.

[193] Graham Meikle, 'Electronic Civil Disobedience and Symbolic Power' in Athina Karatzogianni (ed), *Cyberconflicts and Global Politics* (Routledge, London 2009) 182-3.

[194] Michael E. Gardiner, 'Wild Publics and Grotesque Symposiums: Habermas and Bakhtin on Dialogue, Everyday Life and the Public Sphere' (2004) 52 The Sociological Review 28, 38.

[195] Leah A. Lievrouw, 'Oppositional and Activist New Media: Remediation, Reconfiguration, Participation' (Proceedings of the Ninth Participatory Design Conference, Trento 2006) <http://www.itu.dk/people/kremer/200djs/artikler/p115-lievrouw.pdf> accessed 03 August 2013> 6; Jordan, *Activism!: Direct Action, Hacktivism and the Future of Society* 103;See also culture jamming in Ch 1, Part 1.5 The role of hacktivists as hacker/political entities of counterpower.

[196] Gardiner (194) 39.

[197] Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (Routledge, London 2004) 158.

Naturally, the norms and language of hacktivists could not be fully changed solely through the use of more politically mature rhetoric. However, hacktivists can, at least, demonstrate publicly that they are not only pranksters or socially inconsiderate delinquents, but instead morally conscious, even if not yet fully mature in their political views.[198] In fact, groups before Anonymous, such as EDT or the Electrohippies, had much more concretised political argumentation.[199]

However, the designation and preservation of such normative and tactical safeguards also demonstrates the need for supervision of the use of hacktivist tools and the realisation of their protests. The most appropriate participants for shouldering this responsibility would be the more senior, technically adept hacktivists or groups distributing the tactical software or coordinating less experienced users. Even in self-regulatory models, there must be some form of authority, which could set tactical and moral standards that participants would accept.[200] Although, cyberpolitical movements, such as hacktivist groups, are often ideologically diverse, mobilised masses that mostly converge to fight for specific goals,[201] hacktivist groups, even Anonymous, have some members that are more experienced and are accorded seniority in the relevant online spaces where protesters congregate.[202] Since the legal regime could impose increased responsibility on the organisers of the protests as organising conspirators,[203] community members wishing to avoid serious criminal charges would have to demonstrate a willingness and actual effort to maintain the legitimacy of the acts they organise. Examples of legitimising practice could include the avoidance of destroying code or targeting sites offering infrastructural services, and even potentially an attempt to get permission from the authorities for a virtual sit-in where the law might

[198] Gabriella E. Coleman, 'Anonymous: From the Lulz to Collective Action' (*The New Everyday*, 06 April 2011) <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action> accessed 21 September 2011.

[199] See examples in: DJNZ and The Action Tool Development Group of the Electrohippies Collective, 'Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?' (2001) 34 Leonardo 269*;* Ricardo Dominguez, 'Electronic Disobedience Post-9/11' (2008) 22 Third Text 661.

[200] Jacob van Kokswijk, 'Social Control in Online Society--Advantages of Self-Regulation on the Internet' (International Conference on Cyberworlds, Singapore 2010) 240.

[201] Robert S. Jansen, 'Populist Mobilization: A New Theoretical Approach to Populism' (2011) 29 Sociological Theory 75*,* 82-3.

[202] Eg, Moot is the founder of 4chan and, despite the lack of formal authority, he would be acknowledged as someone many in Anonymous would at least listen to: Adrian Crenshaw, 'Crude, Inconsistent Threat: Understanding Anonymous' (*Irongeek,* 2011) <http://www.irongeek.com/i.php?page=security/understanding-anonymous> accessed 21 September 2011.

[203] See Ch 4 Part 3.3.2 The further criminalisation of inchoate offences.

entail such a provision for offline marches.[204] Efforts to simulate the requirements of offline protests could increase legitimacy by placing the online protests into a publicly familiar, offline context of legitimacy and could potentially be a direction that hacktivists should consider more actively as a legitimising factor. A willingless of hacktivist groups to assess the usefulness and applicability of offline regulations will also demonstrate a willingness to relate to the established norms and interact with other regulators symbiotically in terms of making hacktions more legitimate.

Publicising moral standards and inducing members and supporters to abide by them could also be realised by the integration of those standards into the code-based tools employed during the protests. Since organisers often have control of the code employed for protests, such as virtual sit-in tools or viruses, an important means of preserving legitimacy would be promulgating code that shapes protesters' behaviours accordingly. Principles, such as openness of identity and damage minimisation are already integrated into hacktivist tools in the past.[205] Consequently, self-regulating online collectives could support the use of such tools more persistently and discourage the use of any incompatible protest tools in order to avoid extra-community sanctions.

Moreover, certain identifying code could be integrated into the hacktivist tools employed in order to indicate the purpose of the traffic generated, for example, for virtual sit-in tools like Floodnet. The insertion of identifiable protocols would allow the targets of protests to assess the amount of traffic coming from protesters, thus communicating the extent of public participation of the virtual sit-in in question. Additionally, identifiable code as part of hacktivist tools would allow the differentiation between protest traffic through legitimate, voluntarily-used protest tools, regular traffic by users trying to access the site and debilitating traffic generated by botnets. This, in turn, would be useful for the more proportionate and targeted employment of defensive tools by 'attacked' networks to maintain their functionality, as well as for registering the amount of actual democratically expressed dissent through the use of mainstream hacktivist tools such as virtual sit-in

[204] Hacktivists in Germany resorted to such legitimisation means, such as prior notification and request of permission from the authorities, which played a role in their countering the prosecutor's charges for coercion: see European Digital Rights, 'Frankfurt Appellate Court Says Online Demonstration Is Not Coercion' (*European Digital Rights*, 07 June 2006) <http://www.edri.org/edrigram/number4.11/demonstration> accessed 20 May 2011.

[205] Virtual sit-ins do not mask the identity of users, while viruses employed do not cause undue harms to computer systems. Ch 1, Part 2.2 Hacktivist groups and tactics.

browser applications. The same could be done with viruses in order for code to indicate the origin of the virus and its benign political nature, especially if originating from an identifiable hacktivist group, such as the artistic viruses where the virus' creators even informed cybersecurity firms about their release.[206]

4.3 Identifying deviants and imposing sanctions

Even if supervisory agents can exist, as Murray argues, a community can only regulate itself through the monitoring of consensus and, therefore, defining its membership is a crucial step in these regulatory processes.[207] Regulators should assess whether the moral dictates could actually impact on the casual protesters that will often maintain weak links with the communities, even if deviants could be identified in the first place. Murray warns that communities which lack a particular structure and are formed only on a temporary consensus over specific actions and goals can be so expansive and have such decentralised power structures that community regulation would ultimately be impossible.[208] Hacktivist communities are thus challenged when imposing sanctions such as flaming or banishment from the group,[209] since their members only converge for specific protests, and hence lack a predefined socio-political identity and develop meanings and norms as they evolve.[210]

Considering the above, there seem to be differences between the structural characteristics of regulable communities and the way hacktivist collectives operate. For hacktivists, although a sense of common ideologies and goals might exist within those protesting collectives, political backgrounds and tactical preferences will often vary. The problem of lack of concrete community bonds and membership is also exacerbated by the anonymity often adopted for cyberspace activities. The turn of many online protesters from open identity or traceable pseudonymity to actual anonymity could increase the difficulty

[206] Ch 1, Part 2.2.1 The first era of hacktivism and the birth of electronic civil disobedience.

[207] Murray (n 11) 128.

[208] ibid 163-4.

[209] The most commonly used sanctions would be banishment from the online collectives and strong censure or shaming mechanisms on behalf of the community through public, online criticism (flaming) or the exposition of personal details of the norm-violators, demonstrating the community's disapproval (doxing).

[210] Christian Fuchs, *Internet and Society:Social Theory in the Information Age* (Routledge, New York 2008) 308, 314-5.

of identifying and sanctioning protesters.[211] Consequently, in addition to actually promoting conditions allowing the identification of deviant members, hacktivist communities will have to deal with the question of whether they produce enough links with their members and supporters for any potential sanctions to be possible.

Although, prima facie*,* it appears that hacktivist collectives are totally amorphous and anonymous, there are certain elements that could facilitate, at least to an extent, the identification of members and, thus, also the imposition of sanctions. In the first type of hacktivist groups, those having a specific, identifiable core of organising members, such as the first generation of hacktivist groups, for example, EDT, Electrohippies, Hacktivismo, violation of the group's norms by these core members could have more specific implications. Norm-violation could, for example, mean the expulsion or shaming of the violator by the other group members or the denial of followers to support some of the group's actions, from participation in protests to even publicisation of causes and donations to support the group. Moreover, for such groups with a relatively obvious hierarchy between core organisers and simple participants, most non-organising participants would not be in a position to violate the designated norms, since the parameters of the protests, such as the target, time, duration, notification and tools for the protest would usually be set by the organising protesters.[212] In these cases, the organisers are often an identifiable authority, not so much in the sense of being acknowledged as such, but more in the sense of initiating and coordinating protests and designing the software required. Consequently, sanctions could be imposed in the micro-community of organisers, even if irrelevant for casual participants that lack group attachments. Although, it appears that these core-based political structures could be more easily policed and managed in a self-regulatory mode and would be a preferable structure in terms of legitimisation, the radical responses of the authorities have resulted in further decentralisation/anonymisation, which makes self-policing much more complicated.

[211] Kevin Rawlinson, 'Activists Warned to Watch What They Say as Social Media Monitoring Becomes 'Next Big Thing in Law Enforcement'' (*The Independent*, 01 October 2012) <http://www.independent.co.uk/news/uk/crime/activists-warned-to-watch-what-they-say-as-social-media-monitoring-becomes-next-big-thing-in-law-enforcement-8191977.html> accessed 06 October 2012; Cyrus Farivar, 'NY Judge Compels Twitter to Reveal User's Data' (*Ars Technica,* 02 July 2012) <http://arstechnica.com/tech-policy/2012/07/ny-judge-compels-twitter-to-reveal-user-data/> accessed 02 September 2012.

[212] EDT for example was organising its protests through its ECD webpage calling protesters to participate and setting the standards beforehand. Ricardo Dominguez, 'Electronic Civil Disobedience' *(thing.net,* undated) <http://www.thing.net/~rdom/ecd/ecd.html> accessed 16 January 2011.

However, there could be a way for community sanctions to be employed if efforts are made to more actively exploit existing or develop new points of centralisation within the collective. This could potentially be realised through the use of Internet Relay Chat (iRC) channels, where users interact, or any other website or forum that might constitute a meeting space for hacktivists and supporters. Although participation in those channels can be anonymous, the linking of these channels and the hacktivist collectives to social media could result in many supporters interacting with the groups by logging in using their, often identifiable, social network identities.[213] Even if that is not the case, most users will often adopt pseudonyms that they link to their accounts and are known by them within the online fora. The proliferation and promotion of technologies of identity convergence and portability over various platforms could thus facilitate the identification of participants, at least within the community, since people will use a single identity for their various interactions. The risks for privacy here are important and regulatory actors, such as private online content providers that would manage such projects should make efforts to assure that user identities will not be permeable during the use of their accounts in various online platforms.[214] For the adoption of such measures, stricter controls should be employed regarding surveillance and private information exchanges between private actors and state authorities, so that citizens are not coerced into anonymity to avoid overtly punitive sanctions and undue surveillance.

But even if these convergence projects are not fully adopted and anonymity trends persist, this would not mean that intra-community identification would be impossible, at least for more consistent participants. The online community relations between users could be employed more actively in order for more identification to be facilitated within the community. As Braithwaite argues, anonymity can be a relative concept with intra-community interactions, since members often know more about deviant members and their activities than law-enforcement investigators.[215] Although Braithwaite refers to real-life communities, information made voluntarily available by deviant users bragging to peers

[213] The concept of identity portability, where people can join many networks and websites through their Facebook accounts, for example, is characteristic of this phenomenon and is becoming increasingly popular with many websites offering the opportunity to use one’s established identity from affiliated websites. For the functions and spread of portable identities, see Daniel Kahn, 'Social Intermediaries: Creating a More Responsible Web through Portable Identity, Cross-Web Reputation, and Code-Backed Norms' (2010) 11 Columbia Science & Technology Law Review 176.

[214] ibid.

[215] Braithwaite 'Rules and Principles’ (n 33) 121.

in the groups they frequent[216]or through more traditional online community gossip, could eventually lead community members to identify norm violators. With online communities increasingly emulating real-life ones,[217] community members could potentially uncover the online identities of those disregarding the tactical dictates that each designated action and its organisers might have set for it. Consequently, at least at the level of frequent participants, some sense of identifiability and loose community-building could enable a meaningful imposition of sanctions.[218] Perhaps a more traditional basic group structure would support self-regulation better, but would be very risky in an environment where all identifiable members and particularly organisers are arrested and handed down serious penalties[219] or are coerced into less controversial tactics, such as the case with Dominguez, who was forced to stop organising virtual sit-ins under the threat of prosecution.[220]

An additional regulatory concern is the potential bypassing of community sanctions that are imposed technologically by the sanctioned users. For example, banned members could return under another pseudonym, rendering the penalty essentially ineffective. However, in communities where users have been active for long and have an established status under that name, reappearing with another name could have similar consequences to abandoning one's real-life, assuming, of course, that the user was an active community member. As it has been argued, distinctions between real-life and online communities are artificial[221] and the more our lives are lived online, the more important and similar to real-life communities online communities become.[222] Therefore, expelled users returning with different names will not be able to reconnect with their old contacts and retain their previous group status and, if uncovered, could be banned again. The success of sanctions is, therefore, a matter of

[216] Paul A. Taylor, *Hackers: Crime in the Digital Sublime* (Routledge, London 1999) 6-10; A characteristic example is Mafiaboy, who managed to take large corporate websites offline and was caught after he bragged about it in a hacker forum. See Wikipedia, 'Mafiaboy' (2011) <http://en.wikipedia.org/wiki/MafiaBoy> 11 May 2012.

[217] Murray (n 11) 146-7.

[218] Indicative of the imposition of sanctions is the extensive censuring of one alleged Anonymous member, who presented himself publicly as a spokesperson, thus, violating an important norm of the collective, which prides itself upon not having leaders or official spokesmen: Anonymous (n 188).

[219] The Electrohippies stopped their virtual sit-in and other hacktivist actions due to that fear of high penalties. The Electrohippies Collective 'Cyberlaw UK: Civil Rights and Protest on the Internet' (*iwar.org*, 2000))<http://www.iwar.org.uk/hackers/resources/electrohippies-collective/comm-2000-12.pdf> accessed 15 February 2013.

[220] For details on this case see Evan R. Goldstein, 'Digitally Incorrect' (*The Chronicle Review,* 03 October 2010) <http://chronicle.com/article/Digitally-Incorrect/124649/> accessed 12 August 2011; See also Ch 1, Part 2.2.1 The first era of hacktivism and the birth of electronic civil disobedience.

[221] van Kokswijk (n 200) 239.

[222] Murray (n 11) 146-7.

how important participation in a specific group is for users and also how strict the group is at enforcing its rules. Consequently, expulsion from an online community, even if loosely constituted, will be analogously costlier for frequent rather than casual participants due to the existence of genuine links with other members and the habit of belonging to and interacting with a collective.[223] In that sense, Anonymous would be more of a community than first-era groups, which did not originate from an online community, as Anonymous has from 4chan, thus lacking specific common spaces of convergence, such as the Anonymous iRC channels.

In sum, one could argue that community self-regulation is a challenging prospect for hacktivist collectives, but one that is also primarily important for building an initial normative environment for hacktivists, which entails both preventive and reactive effects. The above discussion establishes that, for self-regulatory mechanisms to work there would at least have to be some form of central gathering space and/or command, and some sense of consistency in participation on behalf of the protesters. Moreover, the more active employment of code within those communities, together with the establishing of more interactive communicative processes between participants could increase the bonds of protesters with the community and facilitate community regulation. For this effort to succeed, the incentivisation of community members to uncover and sanction members, which mar the morality and legitimacy of the protests by disregarding the established norms, is very important.

Considering the difficulties in the self-regulation of hacktivist communities, one of the main reasons that multi-actor approaches have dominated regulatory discussions and have been adopted in this thesis is the fact that no particular, one-sided regulatory solution is absolutely effective on its own. In fact, even the synergy of all the solutions suggested in this chapter would not achieve absolute effectiveness. However, the deficiencies of community self-regulation do not make it undesirable. As Lessig has argued, regulatory controls need not be perfect, since the combination of smaller influences towards the achievement of our goals can provide us with an adequately successful, overall end-result.[224] A basic idea in this chapter is exactly this, that each suggestion on its own, might appear to be insignificant in dealing with the problem, yet it is the synergy of all these

[223] ibid 141-2.

[224] Lessig, *Code v.2.0* (n 32) 73.

efforts that could lead to a more just and efficient regulatory approach for hacktivism. Consequently, one should not be too hasty in condemning self-regulatory solutions as inefficient, despite the serious challenges. Irrespective of the degree of success, community-based regulatory solutions should be encouraged, since they generally facilitate discussion and norm building within and between the online communities, and constitute an important initial level of accountability that educates online activists. Additionally, self-regulatory mechanisms increase the levels of prevention of harmful activities and justify more lenient punishments for hacktivists, avoiding more formal and harmful processes.

5. Conclusion

This chapter has analysed some of the various ways the regulation of hacktivism could be improved and some important conclusions have been drawn in relation to that aim. First, regulation of online phenomena and especially phenomena as complex as hacktivism require the creative and cooperative interplay between all related actors in order improve its regulation. No actor and no method alone could achieve an adequately efficient or just result, be it the state, the hacktivist community or private corporations, since the challenges are overwhelming and require input from many different aspects and contributions from actors with different priorities. All the multiple contributions from all engaged parties in the regulatory effort are important for striking an appropriate balance between respecting morally motivated political activity, moderating hacktions and regulatory excesses against them, achieving efficient prevention of criminal activities and preserving core principles of more general cyberspace governance.

However, perhaps the most important conclusion relevant to achieving a more efficient, just and democratic way to regulate ECD is that it is not a purely criminal activity, nor do we achieve any ultimately beneficial results by treating it as such. As has been seen, hacktivism is a new form of political protest that flows from political struggles that are expressed online and of the technical conditions that inevitably influence the ways this aspect of conflict is realised. Hacktivism in that sense takes the form of the powers it rises against as any resistance does with its generating power, and, thus, if we want a healthier, safer online environment, it is up to power structures and actors to adopt behaviours that reduce tensions and promote legitimacy. This is not one-sided, but it requires concerted effort from all power actors in order for a more harmonious symbiosis to be achieved. After all, as has been seen throughout the thesis, efforts to eliminate hacktivist political expressions have had the opposite effect of propagating and radicalising online protests.

This chapter reinforces the conclusion that some degree of hacktivism will have to be tolerated by democratic legal systems and that suggestions for reform should be based not on elimination, as conflict based approaches aim for, but on a symbiosis that could allow dissent without inducing immoral and harmful incidents. The above realisation could be adequate to induce all engaged actors to eventually work towards facilitating a 'coming together' in striking a sensitive balance between conflicting interests, rather than a 'cracking down' on different opinions. Collaboration, on formal and informal levels, no matter how difficult to achieve in a society with many regulating actors that promote personal interests, could eventually become obvious as a potentially better way forward, not only for hacktivism, but for every conflict in cyberspace. Perhaps the case of hacktivism is an example of the improvements that could be brought about if we substituted coercive for collaborative measures. After all, symbiosis is always better than just monistic survival. In fact, it safeguards survival.

CHAPTER 6
FINAL CONCLUSIONS

Having reached the end of this thesis, it is necessary to highlight the most important points that have been distilled. These can be related back to the core enquiries which have informed the discussion. The first involved the question as to why one should be interested with the regulation of hacktivism. The next was whether the current regulatory framework is working satisfactorily in achieving the desirable goals of security, crime prevention, justice and democratic socio-political organising in relation to the treatment of hacktivism. In essence, this question asked whether the current regime demonstrates any serious deficiencies in regulating hacktivism as something more than criminality. The third major question was whether changing or improving the current regulatory structure to counter these deficiencies is possible and in what ways could western democratic societies move closer to a more functional and desirable model, in accordance with important democratic, utilitarian and deontological concerns.

In relation to these major interrelated questions that underlie the thesis, there have been three major conclusions, which are also causally interrelated and are constituted by smaller conclusions relating not just to hacktivism, but also to more general issues regarding the regulation of cyberspace.

The first complex conclusion has evolved from the chapters analysing the various aspects of hacktivism and its role and importance within cyberspace conflicts of power and the development of the Internet as a social space (chapters 1-3). As has been argued throughout these initial chapters, hacktivism is a consistently existing cluster of practices of political expression in cyberspace which have been practised since its popularisation. Moreover, the analysis has established that, even though hacktivist actions can entail security compromises that would, prima facie at least, be considered criminal, hacktivism has throughout the years also demonstrated characteristics that render it an important socio-political issue to be assessed, not only as a cybersecurity threat, but also in terms of online political organisation and expression. Therefore, hacktivism, even in its less moral and more damaging instances, constitutes an inherent social phenomenon of cyberspace, fusing two intrinsic activities that have been prevalent in cyberspace as a technologically-shaped social space, namely hacking and political activism. Hacktivism has seen different degrees of popularity throughout different eras, with perhaps the most popular and the most chaotic period being the current one, but it has always been a practice of political activity online. Consequently, hacktivism could not be considered a passing trend that, if disregarded, will subside or a trend that can be eliminated through oppression, since it appears to constitute one of the many forms that counterpower can manifest itself against expressive restrictions.

Therefore, hacktivism is significant, not only because of its role in cyberspace as a regulating force within online struggles in addition to being a regulated activity. It is also because it has the potential to be distinguished from plain cybercriminality and can demonstrate a moral character and a political usefulness for networked democracies. The establishment of these special characteristics in relation to hacktivism also provide the analysis with certain criteria and principles that influence the regulatory treatment and potential sanctioning of these activities. These criteria, which relate to its historic and organic role for cyberspace, its ethical and principled background, but also its utility for contemporary democratic online politics, enable and inform the distillation of a list of principles and expectations in relation to how hacktivism should be treated. Answering the second question on the critique and the potential problems the current regulatory regimes might pose for hacktivism and information societies more generally, is based on these principles and criteria extracted from the above analysis of hacktivism.

Consequently, the second major conclusion (contained in chapter four) is that regulating hacktivism is often fraught with problems, inefficiencies and inadequacies in relation to the expectations created from the analysis of the preceding chapters. More particularly, the indiscriminate treatment of hacktivism as the fusion of the negative aspects of political activism and hacking result in treating hacktivists excessively as dangerously criminal and politically subversive on a symbolic and practical level. The current conditions appear to often over-criminalise and excessively punish hacktivists indiscriminately. Laws, norms and political background do not allow criminal justice actors much space for drawing moral and practical distinctions, and hacktivists are indiscriminately condemned, normatively and practically, as criminals or even terrorists. Such perceptions and responses towards hacktivism are intensely expressed through the pervasive political climate and through legislation, as well as through prosecutorial and judicial practices. Additionally, private actors also reinforce the overtly restrictive responses towards hacktivism by promoting or indirectly enforcing more restrictive and illegitimate policies towards politically or technologically controversial expression. On the other hand, private actors make efforts, or are even obliged to abide by the punitive desires of the state, to operate as a private police force and negatively influence hacktivism mainly in terms of the protesters' ablility to organise and gain access to the public through online communications platforms.

Additionally, these over-criminalising and punitive tendencies seem to be generating more injustice and inequality that, in turn, induces more conflict and extreme behaviours from protesters. This vicious cycle of radicalism weakens hacktivists' moral and politically legitimate character. Moreover, the ensuing escalation of punitiveness from the state and radicalisation of protests generates pervasive illegitimacy on both sides of the conflict and increases overall online insecurity. This does not only relate to hacktivists, who adopt less moral practices and are indiscriminately labelled as criminals or dangerous subversives and are punished accordingly. The over-criminalising policies also impact on Internet users in general, whose participation in political collectives and activities is deterred by uncertain legal consequences and prospective high punishments and by the gradual silencing of the more challenging political groups online, which are more prone to face persecution. Furthermore, users' cybersecurity is endangered by the radicalisation and multiplication of hacktivist incidents, which are often done anonymously and take a more vigilantist hue as a response to the intensification of strictness towards hacktivists. The ensuing lack of self-regulation of prospective hacktivists also produces further insecurity and risks for websites, both private and governmental, which are being targeted with more coercive and retaliatory cyberprotests, while the lack of moral and tactical safeguards allows more criminally-minded actors to infiltrate hacktivist collectives for their own purposes.

Drawing from this second conclusion, or cluster of conclusions, the third major conclusion is that there is a need for different approaches towards hacktivism more particularly, but also towards controversial online expression and cyberdeviancy more generally. The realisation flowing from the chapter on the current regulatory conditions is that, even though the Internet is a network of actors that regulate each other, there seems to be a conflict of interests, reinforced by a communicative barrier, between these interacting sides that is the source of most of the negative policies impacting on hacktivism.

The conflicts that propagate the vicious cycle of punitiveness and radicalisation are mainly caused by a lack in understanding of the needs and motives of each side or an unwillingness to do so, which is reinforced by a persistence on conflict rather than an effort to understand causes and effects. These conditions result in each actor resorting to further conflict-inducing responses, rather than to more cooperative and inclusive approaches, based on deliberation and mutual understanding, which would be more consistent with democratic ways of social organising. Acknowledging that hacktivism has taken problematic turns that are particularly encouraged by the propagation of conflict between all stakeholders, the thesis has sought the solution in the adoption of more reconciliatory conceptions of problem-resolution.

Adopting Murray's theory of symbiosis, the thesis suggests that there is a need for a more interactive, multi-actor model of regulating that can only begin to gradually remedy the problems that hierarchical, conflict-bred solutions introduce in a more collaborative and multi-faceted way. Symbiosis is adopted to promote gradual, small changes in various areas in which flaws were identified and to supplement existing, ameliorated responses with novel suggestions as well. These modifications and new suggestions could, gradually and through a concerted effort, impact more justly and effectively on how hacktivism is perceived and treated, promoting more respect and tolerance towards moral practices and finding appropriate measures to deal justly and efficiently with harmful practices.

For this to happen, the first step is to realise that there is a legitimacy deficit in the decision-making and actions of all regulating actors, hacktivists included, that will have to be dealt with in various ways. Primarily, there needs to be an increase in communication processes amongst all stakeholders, with a focus on equality of participation in decision-making and a general increase in the accountability of regulators. Such measures will increase the legitimacy of regulating decisions, be they multi-stakeholder decisions, private policies or new legislative choices.

The second core step identified is the need to introduce ways for tempering the unjustifiable punitiveness of the criminal justice system. This is mainly pursued through suggestions that will facilitate a gradual penal moderation and, more importantly, specialisation through the rationalisation and modernisation of various aspects of criminal justice, from introducing safe harbour provisions to promoting more specialised and socially useful sanctions for cyberdeviants. This is suggested in addition to the promotion of technological education and familiarisation that could slowly impact on normative perceptions and increase our understanding of the interplay of hacktivism with security considerations with the hope of achieving a common understanding amongst those making important regulatory decisions, such as prosecutors, judges and even hacktivists. In essence, it is suggested that the main goal should be the fracturing of the vicious cycle of overregulation and radicalisation. This vicious cycle is the cause of most of the security and right-infringing problems identified in the regulation of hacktivism, since it perpetuates and intensifies illegitimate behaviours on all sides.

However, one should not forget that hacktivists are regulatees and regulators themselves and, therefore, their role in the symbiosis suggested is crucial through efforts that will promote self-regulation. The suggestions on this level are mainly based on creating stronger bonds between users and identifying points of centralisation so that mobilised collectives can perform in more principled and responsible ways that will resemble the first era of hacktivism. Political responsibility from hacktivists, even engendered in the technologies employed, in addition to their arguments and tactical choices would be crucial in portraying a side of hacktivism that could not easily reinforce the efforts of those attempting to delegitimise such practices as criminal or undemocratic. Law-breaking for political purposes requires responsible practices in order for acknowledgment, support and responsible responses to be justifiably demanded from the society and authorities.

Furthermore, the role of private actors, especially as intermediary regulators between state and users, with less stringent controls in their behaviour than those state actors could be forced to accept, is an area where more accountability processes and more interactions with user/subscribers should be promoted. The imposition of policy-making restrictions on the commercial practices of online private intermediaries would be a crucial step in reducing conflict and illegitimacy. Another perspective suggested that could induce symbiosis is private companies using hacktivist protesting against them as indications of the popular acceptability of their policies and a potential need for changes or improvements. Perceiving hacktivist incidents as such, could indicate to companies when their decisions might be too unjust and even counterintuitive even for their own commercial good. Using hacktivism as an ultimate-level dialogic platform between them and users, companies could improve their online policies and services faster and more efficiently and also avoid more radical user confrontations and legal actions in the future. The previous chapter also underlines the crucial role of digital technologies in facilitating these effects, but also the need to maintain a degree of transparency in order to avoid misuses of technological controls by the regulating sides in ways that would promote conflict, instead of openness and communication.

An overarching concern is that the current trends in regulation suggest that a shift towards symbiosis will be hard to promote, since the conflicts are seemingly intensifying. However, the inefficiency of the current approach, in addition to the unjust, over-punitive treatment it can often entail, could gradually induce regulators to reconsider their approach towards hacktivism and also reconsider their general policies towards security and civil liberties, and to engage more interactively with the online community. There have been recent, vivid examples of the influence of users' protesting against SOPA or ACTA that led to their sidelining, at least initially. Mobilising the online community more actively to an extent that policy-makers will have to take account of it, will be a more general victory for online politics, in which hacktivism plays an important role. Even if right-based concerns could not be strong enough to induce a policy reconsideration, security and crime-prevention considerations for the state and corporations could facilitate a gradual realisation of the failure of more punitive and restrictive policies and gradually lead to a shift towards more symbiotic approaches.

The thesis has adopted an optimistic perspective in its suggestions and suggested changes, some minor and some more important without, however, opting for a total break with the current political system or the main principles supporting policy-making. Nonetheless, the analysis does not aim to just reproduce the dominant ideas of the status quo without making an effort to suggest a different route in policy-making within that dominating framework, since as it has been argued such a shift is needed in the case of hacktivism. In order to eventually support a shift in perspectives, empirical research regarding public perceptions about hacktivism and the appropriate ways for regulating such actions will also be required in order to prove some of the arguments made here.

Finally, it is the author's belief that in order to remedy the current situation of a lack of communication between actors and the persistence in following conflict-inducing approaches, the role of academics is crucial, potentially being capable of changing the current conditions and facilitating more understanding and mutually functional interactions. Academics have the potential to actively engage with all actors and adopt the role of a translator/interpreter between regulators/regulatees when they speak different 'languages' and have different normative standards, motives and goals. One could argue that the role of the academic should be one of distant neutrality and, therefore, academics should not actively engage with the regulating actors. My view also advocates neutrality, suggesting, however, an informed, active impartiality, rather than a passive one. More particularly, in the symbiotic environment, the role of the academic is to act as a bridge, interacting on an equal basis with all engaged actors and transferring knowledge and information from one actor to the rest. This process would increase understanding and would facilitate the moderation of actions and policies that evoke tension. In the early stages of symbiosis, when a lack of understanding is more severe, it is important for the academic to attempt to ameliorate tensions by seeking information from all sides and communicating explanations between actors, so that, through the gradual increase of mutual understanding, more functional and fair, symbiotic models could be promoted. After the initial stage of promoting an initial understanding, academics should also put this holistic knowledge gained from their multi-actor interactions into use by also advising or suggesting solutions that each actor could adopt in order to facilitate symbiosis and the goals symbiosis ultimately promotes.

This thesis has involved such a journey of gaining a more holistic understanding of the general framework of hacktivism and its regulation, as well as an attempt to suggest potential improvements for overall security and the promotion of justice and political expression online. It is hoped that this research will serve as guidance for future researchers, policy-makers and even hacktivists in arguing for and implementing a different approach, not only for hacktivism, but also in relation to the wider issue of cybersecurity and Internet rights. The voices of change exist and come from different areas even beyond the hacktivist core. This work has tried to identify these voices and demonstrate how they might facilitate a gradual change in perspectives, acknowledging the difficulties, but also the fact that thinking only based on established norms and perceptions has rarely brought any significant improvement. I hope this thesis has provided the supporters of a different online symbiosis with original theoretical arguments and practical suggestions that could facilitate their efforts and will perhaps also induce critics to reconsider and readjust some of their arguments or shape new, hybrid ones._

BIBLIOGRAPHY

TABLE OF CASES

EUROPEAN COURT OF HUMAN RIGHTS

Appleby v United Kingdom (2003) 37 EHRR 38

Gorzelik and others v Poland (2005) 40 EHRR

KU v Finland (2008) ECtHR 2872/02

GERMANY

OberlandesGericht Frankfurt am Main v Thomas Vogel (No. 1 Ss 319/05)

UNITED KINGDOM

City of London v Samede & Ors [2012] EWHC 34 QB

DPP v Lennon [2006] All ER (D) 147

R v Jones (Margaret) [2005] QB 259

R v Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America [1999] All ER (D) 972

R v Weatherhead, Rhodes, Gibson and Burchall, Southwark Crown Court, 24 January 2013

R v G and Another [2003] UKHL 50

R v Howe [1987] 1 AC 417

R v Ponting [1985] Crim LR 318

R v Saibene and others [2010] Lewes Crown Court

UNITED STATES

Amalgamated Food Employees Union Local 590 v Logan Valley Plaza, Inc., 391 U.S. 308 (1968)

America Online, Inc. v IMS et al. 24 F.Supp.2d 548 (E.D.Va. 1998)

America Online v National Health Care Discount, Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000)

Chicago v Streeter, No. 85-108644 (Cir. Court, Cook County, Ill. 1985)

Citizens United v Federal Election Commission 558 U.S. 310 (2010)

Cyber Promotions, Inc. v America Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996)

EF Cultural Travel BV v Explorica, Inc., 274 F.3d 577 (1st Cir. 2001)

Illinois v Jarka, No. 002170 (Cir. Court Ill. 1985), reprinted in 42 GUILD PRAC. 108–10 (1985)

International Airport Centers, Llc v Citrin, 440 F.3d 418 (7th Cir. 2006)

LVRC Holdings v Brekka, 518 F.3d 1127 (9th Cir. 2009)

Massachusetts v Carter, No. 8745-JC-0091A (Dist. Court, Hampshire County, Mass. 1987)

People of the State of New York v Gray, 150 Misc. 2d 852 (N.Y. Co. 1991)

Register.com, Inc. v Verio, Inc., 126 F.Supp. 2d 238, 255 (S.D.N.Y. 2000)

State v Allen, 917 P.2d 848 (Kan. 1996)

Storage Centers, Inc. v Safeguard Self Storage, Inc., 119 F.Supp. 2d 1121 (Dist. Court, Washington D.C. 2000)

United States v Aguilar, 883 F.2d 662, 693 (9th Cir. 1989)

United States v American Library Association, 539 U.S. 194 (2003)

United States v Auernheimer, Criminal No.: 2:11-cr-470 (SDW) (Dist. Court, New Jersey 2013)

United States v Berrigan, 283 F. Supp. 336 (Dist. Court, Maryland, 1968)

United States v Booker, 543 U.S. 220 (2005)

United States v Cassidy, 616 F.2d 101 (4th Cir. 1979)

United States v Crandon, 173 F.3d 124 (3rd Cir. 1999)

United States v Czubinski, 106 F. 3d 1069 (1st Cir. 1997)

United States v Dorrell, 758 F.2d 427 (9th Cir. 1985)

United States v Guzner, No. 2:09-cr-00087 (Dist. Court, New Jersey 2009)

United States v Heckman, 592 F.3d 400 (3rd Cir. 2010)

United States v Holm, 326 F.3d 872 (7th Cir. 2003)

United States v Kroncke, 459 F.2d 697 (8th Cir. 1972)

United States v Marley, 549 F.2d 561 (8th Cir. 1977)

United States v Maxwell, 254 F.3d 21 (1st Cir. 2001)

United States v May, 622 F.2d 1000 (9th Cir. 1980), cert denied, 449 U.S. 984 (1980)

United States v Mettenbrink, Case 2:09-cr-01149-GAF (Dist. Court, California 2010)

United States v Middleton, 231 F.3d 1207 (9th Cir. 2000)

United States v Mitnick, 145 F.3d 1342 (9th Cir. 1998)

United States v Morris, 928 F.2d 504 (2nd Cir. 1991)

United States v Nosal, 676 F.3d 854 (9th Cir. 2012)

United States v Phillips, 477 F.3d 215 (5th Cir. 2007)

United States v Russell, 600 F.3d 631 (D.C. Cir. 2010)

United States v Schoon, 22 Ill.971 F.2d 193 (9th Cir. 1991)

United States v Sofsky, 287 F.3d 122 (2nd Cir. 2002)

United States v Walser, 275 F.3d 981 (10th Cir. 2001)

United States v White, 244 F.3d 1199 (10th Cir. 2001)

Vermont v Keller, No. 1372-4-84 (Dist. Court, Vt. 1984)

Vermont v McCann, No. 2857-7-86 (Dist. Court, Vt. 1987), reprinted in 44 GUILD PRAC. 101 (1987)

Ward v Rock Against Racism, 491 U.S. 781 (1989)

TABLE OF LEGISLATION

INTERNATIONAL TREATIES, CONVENTIONS AND OTHER DOCUMENTS

Council of Europe, The European Convention for the Protection for Human Rights and Fundamental Freedoms (Rome, 1950)

Council of Europe, Convention on Cybercrime (ETS no.185, Budapest, 2001)

Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ EL 178

Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ L 108

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201

EU Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69

Strafgesetzbuch (German Criminal Code)

UNITED KINGDOM

Anti-Terrorism, Crime and Security Act of 2001 (c. 24)

Coroners and Justice Act 2009 (c.25)

Computer Misuse Act 1990 (c.18)

Criminal Justice Act 2003 (c.44)

Criminal Law Act 1977 (c.45)

Digital Economy Act 2010 (c.24)

Electronic Commerce (EC Directive) Regulations of 2002, No. 2013

Human Rights Act 1998 (c.42)

Magistrates’ Courts Act 1980 (c.43)

Police and Justice Act 2006 (c.48)

Prevention of Terrorism Act 2005 (c.2)

Public Order Act 1986 (c.8)

Terrorism Act 2000 (c.11)

Terrorism Act 2006 (c.11)

The Terrorism Act 2000 (Remedial) Order 2011, No.631

UNITED STATES

Acts of Terrorism Transcending National Boundaries,
18 U.S.C. Part I Chapter 113B, Section 2332b

Animal Enterprise Terrorism Act,
18 U.S.C. Part I, Chapter 3, Section 43

Application of Guidelines in Imposing a Sentence,
18 U.S.C. Chapter 227 Subchapter A. Section 3553(b)

Fraud and Related Activity in Connection with Access Devices,
18 U.S.C. Part I, Chapter 47 Section 1029

Fraud and Related Activity in Connection with Computers,
18 U.S.C. Part I, Chapter 47 Section 1030

Homeland Security Act of 2002,
116 Stat. 2135Homicide,
18 U.S.C. Chapter 51, Section 1111

Identity Theft Enforcement and Restitution Act 2008,
Title II, 122 Stat. 3560

Intelligence Reform and Terrorism Prevention Act of 2004,
118 Stat. 3638

Manslaughter,
18 U.S.C. Chapter 51, Section 1112

Model Penal Code (American Law Institute, 1968)

United States Constitution, Amendment I – Freedom of Religion, Press, Expression

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 - USAPA) 115 Stat. 272

SECONDARY SOURCES

ANONYMOUS WORKS AND ARITHMETIC NAMES

-- 'Immunizing the Internet, Or: How I Learned to Stop Worrying and Love the Worm' (2006) 119 Harvard Law Review 2442

0100101110101101.org, 'Copies' (*0100101110101101.org,* 1999-2000) <http://www.0100101110101101.org/home/copies/index.html> accessed 20 September 2011

-- 'The K Thing: Story of an Infamous Online Performance' (*0100101110101101.org,*2001) <http://www.0100101110101101.org/home> accessed 20 September 2011

-- '0100101110101101.Org Projects' (*0100101110101101.org,*2011) <http://www.0100101110101101.org/projects.html> accessed 26 December 2011

-- 'Contagious Paranoia 0100101110101101.org Spreads a New Computer Virus' (*0100101110101101.org,*2011) <http://www.0100101110101101.org/home/biennale_py/index.html> accessed 26 December 2011

2600 Magazine, 'Press Release - 2600 Magazine Condemns Denial of Service Attacks' (*2600 Magazine,* 10 December 2010) <http://www.2600.com/news/view/article/12037> accessed 27 October 2012

4chan <http://www.4chan.org/> accessed 25 June 2012

A

Aas K F, *Globalization & Crime* (Sage Publications Ltd, London 2007)

Abbas M, 'Economic Crisis Could Widen Inequality - Report' (*Reuters,* 10 October 2010) <http://uk.reuters.com/article/idUKTRE6992CY20101010> accessed 24 October 2010

Adler F, 'Socioeconomic Factors Influencing Jury Verdicts' (1973) 3 New York University Review of Law and Social Change 1

Adler J, *The Urgings of Conscience: A Theory of Punishment* (Temple University Press, Philadelphia 1992)

Agamben G, *Means without End: Notes on Politics* (University of Minnesota Press, Minneapolis 2000)

Akester P, 'Copyright and the P2P Challenge' (2005) 27 European Intellectual Property Review 576

Alexander L, 'Lesser Evils: A Closer Look at the Paradigmatic Justification' (2005) 24 Law and Philosophy 611

Alexander L, Kessler K F and Morse S J, *Crime and Culpability: A Theory of Criminal Law* (Cambridge University Press, Cambridge 2009)

Ali M 'Anonymous, the Wikileaks Defenders Clarify: We Are Not Hackers, We Won't Steal Your Credit Cards' (*Geekword,* 11 December 2010) <http://www.geekword.net/anonymous-pr/> accessed 16 January 2011

All Party Internet Group (APIG) 'Revision of the Computer Misuse Act': Report on an inquiry by the All Party Internet Group (2004) <http://www.cullen-international.com/cullen/multi/national/uk/laws/cmareport.pdf> accessed 14 August 2013

Allan G, 'Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative' (2005) New Zealand Law Review 149

Allnutt L 'Old-School Hacker Oxblood Ruffin Discusses Anonymous and the Future of Hacktivism' (*Tangled Web*, 08 June 2011) <http://www.rferl.org/content/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html> accessed 20 September 2011

Alschuler A, 'Implementing the Criminal Defendant's Right to Trial: Alternatives to the Plea Bargaining System' (1983) 50 University of Chicago Law Review 931

Alton S R, 'In the Wake of Thoreau: Four Modern Legal Philosophers and the Theory of Non-Violent Civil Disobedience' (1993) 24 Loyola University Law Journal 39

Amnesty International,'Undermining Freedom of Expression in China: The Role of Yahoo!, Microsoft and Google' (*Amnesty International*, 2006) <http://web.amnesty.org/library/pdf/POL300262006ENGLISH/$File/POL3002606.pdf> accessed 20 May 2012

Anderson N, 'Germany Adopts "Anti-Hacker" Law; Critics Say It Breeds Insecurity' (*ArsTechnica*, 28 May 2008 <http://arstechnica.com/security/news/2007/05/germany-adopts-anti-hacker-law-critics-say-it-breeds-insecurity.ars> accessed 20 May 2011

-- 'US Net Neutrality Rules Finalized, in Effect November 20' (*ArsTechnica,* 22 September 2011) <http://arstechnica.com/tech-policy/2011/09/us-net-neutrality-rules-finalized-in-effect-november-20/> accessed 30 August 2012

Androulakis N, *Penal Law: General Part* (P.N. Sakkoulas, Athens 2000)

Anonymous 'Teenage Hacker Admits Scientology Cyber-Attack USA v. Guzner – Information' (*Secretdox*, 18 October 2008) <http://secretdox.wordpress.com/2008/10/18/usa-v-guzner-plea-agreement-for-defendant-dmitriy-guzner/> accessed 20 May 2011

-- 'Protest in the Digital Era: DDoS and the Online Sit-In' (*Truthisrevolutionary*, 16 December 2010) <http://truthisrevolutionary.org/news/protest-digital-era-ddos-and-online-sit> accessed 20/05/2011

-- 'Anonymous - Code of Conduct' (*YouTube*, 21 December 2010) <https://www.youtube.com/watch?v=-063clxiB8I> accessed 16 February 2013

-- 'Anonymous Declaration of Freedom' *(Whyweprotest*, 10 January 2011) <http://www.whywefight.net/2011/01/10/anonymous-declaration-of-freedom/#axzz2HrN1bzrV> accessed 10 January 2011

-- 'Anonymous Press Release: Open Letter from Anonymous to the UK Government' (*Anonops*, 27 January 2011) <http://anonops.webs.com/ANONYMOUS-PRESS-RELEASE_27-01-2011.pdf> accessed 10 November 2012

-- 'Everything Anonymous' (*Anonnews,* 08 March 2011) <http://anonnews.org/?p=comments&c=ext&i=996> accessed 30 August 2012

-- 'Anonymous Is Not Unanimous' (*Pastebin,* 17 August 2011) <http://pastebin.com/4vprKdXH> accessed 20 December 2011

-- 'Everything Anonymous' (*AnonNews,* 08 March 2011) <http://anonnews.org/?p=comments&c=ext&i=996> accessed 30 August 2012

Anonymous Interviewer 'Fragmented Plurality: An Interview with Gabriella Coleman' (*The Breaking Time,* 14 April 2011) <http://thebreakingtime.typepad.com/the_breaking_time/2011/04/an-enormous-plurality-an-interview-with-gabriella-coleman.html> accessed 20 May 2011

Arendt H, *Crises of the Republic* (4th edn, Harvest Books, San Diego 1972)

Aronowitz S and Gautney H (eds), *Implicating Empire: Globalization and Resistance in the 21st Century World Order* (Basic Books, New York 2003)

Arthur C 'Inside 'Anonymous': Tales from within the Group Taking Aim at Amazon and Mastercard' (*The Guardian Technology Blog*, 13 December 2010) <http://www.guardian.co.uk/technology/blog/2010/dec/13/hacking-wikileaks> accessed 19 December 2012

-- 'Lulzsec: What They Did, Who They Were and How They Were Caught' (*The Guardian Technology Blog,* 16 May 2013) <http://www.guardian.co.uk/technology/2013/may/16/lulzsec-hacking-fbi-jail> accessed 20 June 2013

Ashford W, 'Infosec 2013: Cyber Crime Challenges Law Enforcement' (*Computer Weekly,* 25 April 2013) <http://www.computerweekly.com/news/2240182575/Infosec-2013-Cyber-crime-challenges-law-enforcement> accessed 20 June 2013

Ashworth A, *Sentencing and Penal Policy* (Weidenfeld and Nicolson, London 1983)

-- 'Some Doubts About Restorative Justice' (1993) 4 Criminal Law Forum 277

-- 'Is the Criminal Law a Lost Cause?' (2000) 116 Law Quarterly Review 225

Ashworth A and Player E 'Sentencing, Equal Treatment and the Impact of Sanctions' in Ashworth A and Wasik M (eds), *Fundamentals of Sentencing Theory* (Clarendon Press, Oxford 1998)

Aspen Institute, 'ASF 2011 Cyber-Security' (Aspen Security Forum Proceedings, *YouTube,* 29 July 2011) <http://www.youtube.com/watch?v=yoWkAVXmSs0> accessed 31 July 2013

Astier S, 'Ethical Regulation of the Internet: The Challenges of Global Governance' (2005) 71 International Review of Administrative Sciences 133

Ayres I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, New York 1995)

B

Badiou A, *Metapolitics* (Jason Barker tr,Verso, London 2005)

Baggini J 'England Riots: Are Harsh Sentences for Offenders Justified?' (*The Guardian*, 17 August 2011) <http://www.guardian.co.uk/uk/2011/aug/17/england-riots-harsh-sentences-justified> accessed 08 September 2011

Bainbridge D I, *Introduction to Information Technology Law* (6th edn, Pearson Education Limited, Essex 2007)

Baldwin R, *Rules and Government* (Clarendon Press, Oxford 1995)

Baldwin R and Black J, 'Really Responsive Regulation' (2008) 71 The Modern Law Review 59

Ball J 'By Criminalising Online Dissent We Put Democracy in Peril' (*The Guardian,* 01 August 2011 <http://www.guardian.co.uk/commentisfree/2011/aug/01/online-dissent-democracy-hacking> accessed 21 September 2011

Barbwise M, 'Google Scanning - Is It Legal?.' (*H-Online,* 20 February 2008) <http://www.h-online.com/security/features/Google-scanning-is-it-legal-746155.html,> accessed 29 October 2010

Bauman Z, *Modernity and Ambivalence* (Polity Press, Cambridge 1991)

Bazelon D L, Choi Y J, and Conaty J F, 'Computer Crimes' (2006) 43 American Criminal Law Review 259

Bazzichelli T, *Networking: The Net as Artwork* (*Digital Aesthetics Research Center*, Aarhus University, Aarhus 2008)

BBC 'The Cyber Raiders Hitting Estonia' (*BBC*, 17 May 2007) <http://news.bbc.co.uk/1/hi/world/europe/6665195.stm> accessed 24 October 2010

-- 'Email and Web Use 'to Be Monitored' under New Laws' (*BBC,* 01 April 2012) <http://www.bbc.co.uk/news/uk-politics-17576745> accessed 15 April 2012

-- 'The Pirate Bay Must Be Blocked by Uk ISPs, Court Rules' (*BBC,* 30 April 2012 <http://www.bbc.co.uk/news/technology-17894176> accessed 29 May 2012

-- 'Dutch Court Bans Pirate Party Links to the Pirate Bay' (*BBC,* 10 May 2012 <http://www.bbc.co.uk/news/technology-18016819> accessed 29 May 2012

-- 'Gary Mckinnon Extradition to US Blocked by Theresa May' (*BBC*, 16 October 2012) <http://www.bbc.co.uk/news/uk-19957138> accessed 10 November 2012

-- 'Anonymous Hackers 'Cost Paypal £3.5m'' (*BBC*, 22 November 2012) <http://www.bbc.co.uk/news/uk-20449474> accessed 24 November 2012

Beale S S, 'What's Law Got to Do with It? The Political, Social, Psychological and Non-Legal Factors Influencing the Development of (Federal) Criminal Law' (1997) 1 Buffalo Criminal Law Review 23

-- 'The News Media's Influence on Criminal Justice Policy: How Market-Driven News Promotes Punitiveness' (2006) 48 William & Mary Law Review 397

Bedau H A, 'Civil Disobedience and Personal Responsibility for Injustice' (1970) 54 The Monist 517

-- 'Civil Disobedience in Focus: Introduction' in Bedau H A (ed), *Civil Disobedience in Focus* (Routledge, London 2002)

Benkler Y, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press, London 2006)

Bentham J, 'Introduction to the Principles of Morals and Legislation' in Alan Ryan (ed), *John Stuart Mill and Jeremy Bentham: Utilitarianism and Other Essays* (Penguin Group, London 1824)

Biancuzzi F 'Achtung! New German Laws on Cybercrime' (*Security Focus*, 10 July 2007 <http://www.securityfocus.com/columnists/448> accessed 20 May 2011

Bickel A M, 'Civil Disobedience and the Duty to Obey' (1973) 8 Gonzaga Law Review 199

Biegel S, *Beyond Our Control?: Confronting the Limits of Our Legal System in the Age of Cyberspace* (The MIT Press, London 2003)

Bix B, *Jurisprudence: Theory and Context* (5th edn, Thomson Reuters (Legal) Limited, London 2009)

Black J, 'Constitutionalising Self-Regulation' (1996) 59 The Modern Law Review 24

-- 'Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a" Post-Regulatory" World' (2001) 54 Current Legal Problems 103

-- 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1

-- 'Proceduralisation and Polycentric Regulation' (2005) Especial 1 RevistaDIREITOGV <http://direitogv.fgv.br/sites/direitogv.fgv.br/files/rdgv_esp01_p099_130.pdf> accessed 16 December 2012

Black T, 'Hacktivism: The Poison Gas of Cyberspace' (*Spiked-Online,* 14 Decemeber 2010) <http://www.spiked-online.com/index.php/site/article/10001/> accessed 14 December 2010

Blackstone W T, 'Civil Disobedience: Is It Justified?' (1969) 3 Georgia Law Review 679

Bliss J and Blum J 'Holder Says U.S. Probes Wikileaks-Related Web Attacks' (*Bloomberg,* 09 December 2010) <http://www.bloomberg.com/news/2010-12-09/holder-says-u-s-is-looking-into-wikileaks-tied-cyber-attacks.html> accessed 16 January 2011

Borradori G, *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Jacques Derrida* (University of Chicago Press, Chicago 2003)

Bowling B, Marks A, and Murphy C C, 'Crime Control Technologies: Towards an Analytical Framework and Research Agenda', in Brownsword R and Yeung K (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008)

Boyd C 'Estonia Open Politics to the Web' (news.bbc.co.uk, 07 May 2004) <http://news.bbc.co.uk/1/hi/technology/3690661.stm> accessed 24 October 2010

-- 'Profile: Gary Mckinnon' *(BBC*, 30 July 2008) <http://news.bbc.co.uk/1/hi/technology/4715612.stm> accessed 30 May 2012

Boyd L 'The Yes Men and Activism in the Information Age'(MA Thesis, Louisiana State University and Agricultural and Mechanical College 2005)

Braithwaite J, 'Rules and Principles: A Theory of Legal Certainty' (2002) 27 Australian Journal of Legal Philosophy 47

-- *Restorative Justice and Responsive Regulation* (Oxford University Press, Oxford 2002)

Braun S et al. 'Secret to Prism Program: Even Bigger Data Seizure' (*Associated Press,* 15 June 2013) <http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure> accessed 21 June 2013

Brenner S W, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' (2007) 97 Journal of Criminal Law & Criminology 379

-- *Cybercrime: Criminal Threats from Cyberspace* (Praeger Publishers, Oxford 2010)

Brody S R, 'The Effectiveness of Sentencing: A Review of the Literature (Home Office Research Study No.35, Home Office Research Unit, London 1976)

Brown Jr S M, 'Civil Disobedience' (1961) 58 The Journal of Philosophy 669

Brownlee K, 'The Communicative Aspects of Civil Disobedience and Lawful Punishment' (2006) 1 Criminal Law and Philosophy Journal 179

-- 'Justifying Punishment: A Response to Douglas Husak' (2008) 2 Criminal Law and Philosophy 123

-- 'Civil Disobedience' (*Stanford Encyclopedia of Philosophy*, 23 December 2009) <http://www.illc.uva.nl/~seop/entries/civil-disobedience/> accessed 12 August 2011

Buckland B S, Schreier F and Winkler T H,'Democratic Governance Challenges of Cyber Security' (DCAF Horizon 2015 Working Paper No. 1, *Geneva Security Forum,* 2012) <http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf> accessed 15 May 2013

Burris S, Kempa M, and Shearing C, 'Changes in Governance: A Cross-Disciplinary Review of Current Scholarship', (2008) 41 Akron Law Review 1

Burstein P, 'The Impact of Public Opinion on Public Policy: A Review and an Agenda' (2003) 56 Political Research Quarterly 29

C

Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* (London 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 03 August 2013

Cahill M, 'Punishment Decisions at Conviction: Recognizing the Jury as Fault-Finder' (2005) University of Chicago Legal Forum 91

Calabrese A (2004) 'Virtual Nonviolence? Civil Disobedience and Political Violence in the Information Age' 6 info <www.emeraldinsight.com/1463-6697.htm > accessed 15 June 2010

Calkins M M, 'They Shoot Trojan Horses, Don't They-an Economic Analysis of Anti-Hacking Regulatory Models' (2000) 89 Georgia Law Journal 171

Callinicos A 'The Anti-Capitalist Movement after Genoa and New York', in Arownowitz S and Gautney H (eds), *Implicating Empire: Globalization and Resistance in the 21st Century World Order* (New York Basic Books 2003)

Cashell B et al. (2004), 'CRS Report for Congress: The Economic Impact of Cyber-Attacks'.

Cassim F, 'Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study' (2009) 12 Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad 35

Castells M, *Information Age, Economy, Society and Culture* (Blackwell, Oxford 1996)

-- 'Informationalism, Networks, and the Network Society: A Theoretical Blueprint' in Castells M (ed), *The Network Society: A Cross Cultural Perspective* (Edward Elgar Publishing Limited, Cheltenham 2004)

-- *Communication Power* (Oxford University Press, Oxford 2009)

Castle N, 'Internet Art and Radicalsim in the Digital Culture Industry' (2000) <http://www.lulu.com/items/volume_1/89000/89324/2/preview/netart_preview.pdf> accessed 16 June 2011

Castronova E, *Synthetic Worlds: The Business and Culture of Online Games* (University of Chicago Press, Chicago 2005)

Cavallaro J L, 'The Demise of the Political Necessity Defense: Indirect Civil Disobedience and United States v. Schoon' (1993) 81 California Law Review 351

Centre for the Protection of National Infrastructure 'The National Infrastructure' (undated) <http://www.cpni.gov.uk/about/cni/> accessed 20 June 2013

Choi B H, 'The Grokster Dead-End' (2005) 19 Harvard Journal of Law & Technology 393

Christensen H S (2011) 'Political Activities on the Internet: Slacktivism or Political Participation by Other Means?' 16 First Monday <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3336/2767> accessed 17 December 2012

Christie G C, 'Lawful Departures from Legal Rules: "Jury Nullification" and Legitimated Disobedience', (1974) 62 California Law Review 1289

Christopher R L, 'The Prosecutor's Dilemma: Bargains and Punishments' (2003) 72 Fordham Law Review 93

CISCO 'Combating Botnets Using the Cisco Asa Botnet Traffic Filter' (*CISCO White Paper,* 2009) <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/white_paper_c11-532091.html> accessed 26 February 2012

Clarkson C M V, Keating H M, and Cunningham S R, *Criminal Law: Text and Materials* (7th edn, Thomson Reuters Ltd, London 2010)

Clinton A C, 'Taming the Hydra: Prosecutorial Discretion under the Acceptance of Responsibility Provision of the Us Sentencing Guidelines' (2012) 79 The University of Chicago Law Review 1467

Cody J A, 'Derailing the Digitally Depraved: An International Law and Economics Approach to Combating Cybercrime & Cyberterrorism' (2002) 11 MSU DCL Journal of International Law 231

Cohan J A, 'Civil Disobedience and the Necessity Defense' (2007) 6 Pierce Law Review 111

Cohen A, 'Case Study: The Supreme Court and Corporate Free Speech' (*Time,* 07 July 2010) <http://www.time.com/time/nation/article/0,8599,2001844,00.html> accessed 21 December 2012

Cohen C, 'Civil Disobedience and the Law' (1966) 21 Rutgers Law Review 1

Cohen S, *Folk Devils and Moral Panics* (Paladin, St Albans 1973)

Colby C P, 'Civil Disobedience: A Case for Separate Treatment' (1968) 14 Wayne Law Review 1165

Coleman G E 'Anonymous: From the Lulz to Collective Action' (*The New Everyday*, 06 April 2011 <http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action>, accessed 21 September 2011.

Colon M 'RSA Conference 2012: Hacktivism Forcing Organizations to Look Inward' (*SC Magazine*, 29 February 2012 <http://www.scmagazine.com/rsa-conference-2012-hacktivism-forcing-organizations-to-look-inward/article/230051/> accessed 10 November 2012.

Columbia Law Review Association 'Sentencing in Cases of Civil Disobedience' (1968) 68 Columbia Law Review 1508

Council on Crime and Justice, *The Collateral Effects of Incarceration on Fathers, Families, and Communities* (Research Demonstration Advocacy, 2006)< http://www.racialdisparity.org/files/CEI%20FINAL%2003312006.pdf> accessed 15 February 2013

Couts A, 'US Gov't Ramps up Anti-Anonymous Rhetoric, Warns of Power Grid Take-Down' (*Digital Trends,* 12 February 2012) <http://www.digitaltrends.com/web/us-govt-ramps-up-anti-anonymous-rhetoric-warns-of-power-grid-take-down/> accessed 20 June 2013

Crawford A 'Policing and Security as 'Club Goods': The New Enclosures', in Wood J and Dupont B (eds), *Democracy, Society and the Governance of Security* (Cambridge Cambridge University Press 2006)

Crenshaw A, 'Crude, Inconsistent Threat: Understanding Anonymous' (*Irongeek,* 2011) <http://www.irongeek.com/i.php?page=security/understanding-anonymous> accessed 21 September 2011

Criminal Justice Alliance,'Crowded Out: The Impact of Prison Overcrowding on Rehabilitation' (*The Criminal Justice Alliance,* 2012) <http://www.criminaljusticealliance.org/Crowded_Out_CriminalJusticeAlliance.pdf> accessed 20 June 2013

Critical Art Ensemble *Electronic Disturbance* (Autonomedia, New York 1993) <http://www.critical-art.net/books.html> accessed 31 July 2013

-- *Electronic Civil Disobedience and Other Unpopular Ideas* (Autonomedia, New York 1996) <http://www.critical-art.net/books.html> accessed 31 July 2013

-- *Digital Resistance* (Autonomedia, New York 2001) <http://www.critical-art.net/books.html> accessed 31 July 2013

Cross F B, 'Decisionmaking in the US Circuit Courts of Appeals' (2003) 91 California Law Review 1475

CrossTalk, 'From Hacktivism to Wikiwarfare' (*RT,* uploaded 17th Decemeber 2010) <http://www.youtube.com/watch?v=mFJa9RHAfOk> accessed 17 December 2010

Crown Prosecution Service, 'Appeals: Judicial Review of Prosecutorial Decisions' (2009) <http://www.cps.gov.uk/legal/a_to_c/appeals_judicial_review_of_prosecution_decisions/> accessed 24 November 2012

Crown Prosecution Service, 'The Code for Crown Prosecutors' (2010) <http://www.cps.gov.uk/publications/code_for_crown_prosecutors/> accessed 15 February 2013

Cullen F, Fisher B, and Applegate B, 'Public Opinion About Punishment and Corrections' (2000) 27 Crime and Justice 1

D

Dagger R J, *Civic Virtues: Rights, Citizenship, and Republican Liberalism* (Oxford University Press, New York 1997)

Dampier P '300,000 Protest Verizon-Google Net Neutrality Pact' (stopthecap.com, 10 August 2010) <http://stopthecap.com/2010/08/10/300000-protest-verizon-google-net-neutrality-pact/>, accessed 31 May 2012

Danidou Y and Schafer B, 'In Law We Trust? Trusted Computing and Legal Responsibility for Internet Security' (2009) Emerging Challenges for Security, Privacy and Trust 399

Davies H and Holdcroft D, *Jurisprudence: Text and Commentary* (Butterworths & Co Ltd, London 1991)

Davis A J, *Arbitrary Justice: The Power of the American Prosecutor* (Oxford University Press, Oxford 2007

Davis M, 'How to Make the Punishment Fit the Crime' (1983) 93 Ethics 726

De Silva S and Weedon F, 'A Future Less Certain for the Digital Economy Act?' (2011) 17 Computer and Telecommunications Law Review 149

De Villiers M, 'Distributed Denial of Service: Law, Technology & Policy' (2007) University of New South Wales Faculty of Law Research Series, Paper 7, 1

Decker C, 'Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime' (2007) 81 South California Law Review 959

DeForrest M E, 'Civil Disobedience: Its Nature and Role in the American Legal Landscape' (1998)33 Gonzaga Law Review 653

Denning D E, 'Hacktivism: An Emerging Threat to Diplomacy' (2000) 77 Foreign Service Journal 43

-- 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in Arquila J and Ronfeldt D (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND Corporation 2001)

Department of Homeland Security, 'National Infrastructure Protection Plan: Information Technology Sector' (undated) <http://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-information-technology-snapshot-2011.pdf> accessed 30 August 2012

Devine D J et al., 'Jury Decision Making: 45 Years of Empirical Research on Deliberating Groups', (2000) 7 Psychology, Public Policy and Law 622

Dictionary.com 'Protest' (2012) <http://dictionary.reference.com/browse/protest> accessed 25 January 1013

DJNZ and The Action Tool Development Group of the Electrohippies Collective, 'Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?' (2001)34 Leonardo 269

Dominguez R 'Electronic Civil Disobedience in Solidarity with Greek Anarchists' (*thing.net*, 2008) <http://post.thing.net/node/2457> accessed 19 December 2011

-- 'Electronic Disobedience Post-9/11' (2008) 22 Third Text 661

-- 'FBI has ended the "Investigation" of Vr Sit-in Performance' (*b.a.n.g*, 12 November 2010) <http://bang.calit2.net/2010/11/fbi-has-ended-the-“investigation”-of-vr-sit-in-performance/> accessed 20/05/2011

-- 'Electronic Civil Disobedience' (*thing.net*, undated) <http://www.thing.net/~rdom/ecd/ecd.html> accessed 16 January 2011

Dotan Y, 'Should Prosecutorial Discretion Enjoy Special Treatment in Judicial Review?: A Comparative Analysis of the Law in England and Israel' (1997) 3 Public Law 513

Dotcom K, 'Prism: Concerns over Government Tyranny Are Legitimate' (*The Guardian,* 13 June 2013) <http://www.guardian.co.uk/commentisfree/2013/jun/13/prism-utah-data-center-surveillance> accessed 21 June 2013

Dowland P et al., 'Computer Crime and Abuse: A Survey of Public Attitudes and Awareness' (1999) 18 Computers & Security 715

Doyle C, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws* (Congressional Research Service, Report for Congress, DIANE Publishing, 2011)

Duff A, *Punishment, Communication, and Community* (Oxford University Press, Oxford 2001)

Dutton W H et al., *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* (UNESCO, Oxford 2010)

Dworkin R, 'The Model of Rules' (1967) 35 University of Chicago Law Review 14

-- *Taking Rights Seriously* (2nd edn, Harvard University Press, Cambridge(Ma) 1978)

-- *A Matter of Principle* (Harvard University Press, Cambridge (Ma) 1985)

E

Eatwell R, 'Community Cohesion and Cumulative Extremism in Contemporary Britain' (2006) 77 The Political Quarterly 204

Electronic Frontier Foundation 'Letter to Governor Pataki' (*Electronic Frontier Foundation,* 12 March 2003) <https://w2.eff.org/Privacy/TIA/20030314_letter_to_pataki.php> accessed 12 July 2012

Ely A N, 'Prosecutorial Discretion as an Ethical Necessity: The Ashcroft Memorandum's Curtailment of the Prosecutor's Duty to Seek Justice' (2004) 90 Cornell Law Review 237

Engle E (2011) 'The Rights' Orchestra: Proportionality, Balancing, and Viking' New England Journal of International Law and Comparative Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1704503> accessed 31 January 2012

EpidemiC 'Antimafia: The Action Sharing' (EpidemiC.ws, 2002) <http://epidemic.ws/antimafia/action.php?lng=en> accessed 20 September 2011

Epstein D, 'The Duality of Information Policy Debates: The Case of the Internet Governance Forum' (DPhil, Cornell University 2012)<http://core.kmi.open.ac.uk/display/6103666> accessed 13 June 2013

Epstein R A, 'Cybertrespass' (2003) 70 The University of Chicago Law Review, Centennial Tribute Essays 73

Eriksson J and Giacomello G, 'The Information Revolution, Security, and International Relations:(Ir) Relevant Theory?' (2006) 27 International Political Science Review 221

European Data Protection Supervisor 'Opinion of the European Data Protection Supervisor: On Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data' (*EDPS*, Brussels 2007) <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf> accessed 13 May 2013

European Digital Rights 'Frankfurt Appellate Court Says Online Demonstration Is Not Coercion' (*European Digital Rights*, 07 June 2006) <http://www.edri.org/edrigram/number4.11/demonstration> accessed 20 May 2011

European Network and Information Security Agency (ENISA) 'Sweden Country Report' (*ENISA*, 2011) <http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Sweden.pdf> accessed 15 February 2013

F

Fafinski S, 'The Security Ramifications of the Police and Justice Act 2006' (2007) Network Security 8

-- 'Computer Misuse: The Implications of the Police and Justice Act 2006' (2008) 72 Journal of Criminal Law 53

Farivar C, 'NY Judge Compels Twitter to Reveal User's Data' (*ArsTechnica*, 02 July 2012) <http://arstechnica.com/tech-policy/2012/07/ny-judge-compels-twitter-to-reveal-user-data/> accessed 02 September 2012

Farrell D, 'Paying the Penalty: Justifiable Civil Disobedience and the Problem of Punishment' (1977) 6 Philosophy & Public Affairs 165

Federal Communications Commission 'Preserving the Open Internet - Broadband Industry Practices' (Federal Communications Commission Report, 2010)

Feinberg J, *'Harm to Others: The Moral Limits of the Criminal Law, Vol. 1'* (Oxford University Press, Oxford 1984)

Fiedler S, 'The Right to Rebel: Social Movements and Civil Disobedience' (2009) 1 Cosmopolitan Civil Societies Journal 42

Finklea K and Theohary C,'CRS Report for Congress: Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement' (*Congressional Research Service*, 2013) <http://www.fas.org/sgp/crs/misc/R42547.pdf > accessed 04 May 2013

Finman T and Macaulay S, 'Freedom to Dissent: The Vietnam Protests and the Words of Public Officials' (1966) Wisconsin Law Review 632

Finnis J, *Natural Law and Natural Rights* (Oxford University Press, Oxford 2011)

Fitzpatrick A, 'Wikileaks Wins Battle against Visa, Mastercard' (*Mashable,* 12 July 2012) <http://mashable.com/2012/07/12/wikileaks-wins-battle-against-visa-mastercard/> accessed 10 June 2013

Fletcher G P, *Basic Concepts of Criminal Law* (Oxford University Press, New York 1998)

Forte D M 'Is "Virtual" Activism Not "Real" Activism' (*Cyberspace Ethnography: Political Activism and the Internet Blog*, 29 January 2010) <http://webography.wordpress.com/2010/01/29/is-virtual-activism-not-real-activism/> accessed 20 May 2011

Foucault M 'Prison Talk ' in Gordon C (ed), *Power/Knowledge* (Brighton Harvester 1980)

-- *The Will to Knowledge: The History of Sexuality* (Penguin, London 1998)

Fox L 'From Hacktivists to Spammers: Is Anonymous Failing?' (newsjunkiepost.com, 12 December 2010) <http://newsjunkiepost.com/2010/12/12/from-hacktivists-to-spammers-is-anonymous-failing/> accessed 28 September 2011.

Freeman J, 'Real Democracy Problem in Administrative Law' in Dyzenhaus D (ed), *Recrafting the Rule of Law* (Hart Publishing, Oxford 1999)

Froomkin M, 'Habermas@ Discourse. Net: Toward a Critical Theory of Cyberspace' (2003) 116 Harvard Law Review 749

Frydman B and Rorive I, 'Regulating Internet Content through Intermediaries in Europe and the USA' (2002) 23 Zeitschrift für Rechtssoziologie 41

Fuchs C, *Internet and Society: Social Theory in the Information Age* (Routledge, New York 2008)

Fuller L, *The Morality of Law* (Revised edn, Yale University Press, New Haven 1969)

Furnham A, McClelland A, and Baxter E D, 'The Allocation of a Scarce Correctional Resource: Deciding Who Is Eligible for an Electronic Monitoring Program' (2010) 40 Journal of Applied Social Psychology 1606

G

Gardbaum S, 'The Horizontal Effect of Constitutional Rights' (2003) 102 Michigan Law Review 387

Gardiner M E, 'Wild Publics and Grotesque Symposiums: Habermas and Bakhtin on Dialogue, Everyday Life and the Public Sphere' (2004) 52 The Sociological Review 28

Gardner J 'Crime: In Proportion and in Perspective ', in Ashworth A and Wasik M (eds), *Fundamentals of Sentencing Theory* (Clarendon Press, Oxford 1998)

Garfield B, 'In Defense of DDoS' (Transcript of Interview with Evgeny Morozov, *On the Media,* 17 December 2010) <http://www.onthemedia.org/transcripts/2010/12/17/02> accessed 20 May 2011

Garland D, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford University Press, Oxford 2001)

Gillett G, 'A World without Internet: A New Framework for Analyzing a Supervised Release Condition That Restricts Computer and Internet Access' (2010) 79 Fordham Law Review 217

Gilroy A A, 'CRS Report for Congress: Net Neutrality: Background and Issues' (Congress Research Service, 2008) <http://www.fas.org/sgp/crs/misc/RS22444.pdf> accessed 13 June 2013

Global Research, 'U.S. Social Inequality Income Gap Hits Record High' (*Market Oracle*, 29 September 2010) <http://www.marketoracle.co.uk/Article23088.html> accessed 24 October 2010

Goldsmith J and Wu T, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press, Oxford 2006)

Goldsmith J L, 'Against Cyberanarchy', (1998) 65 The University of Chicago Law Review 1199

Goldstein E R 'Digitally Incorrect' (*The Chronicle Review,* 03 October 2010) <http://chronicle.com/article/Digitally-Incorrect/124649/> accessed 12 August 2011

Goldstein N, 'Steubenville's Tangled Web of Injustice' (*The Guardian,* 12 June 2013) <http://www.guardian.co.uk/commentisfree/2013/jun/12/steubenville-tangled-web-injustice> accessed 21 June 2013

Graber C B, 'Internet Creativity, Communicative Freedom and a Constitutional Rights Theory Response to "Code Is Law"' (Lucerne i-call, The Research Centre for International Communications and Art Law, University of Lucerne, Working Paper 03, 2010)

Granick J, 'Faking It: Calculating Loss in Computer Crime Sentencing' (2005) 2 I/S: A Journal of Law and Policy 207

Green N and Halliday J 'Twitter Unmasks Anonymous British User in Landmark Legal Battle' (*The Guardian*, 29 May 2011) <http://www.guardian.co.uk/technology/2011/may/29/twitter-anonymous-user-legal-battle> accessed 02 September 2012

Greenawalt K, 'A Contextual Approach to Disobedience' (1970) 70 Columbia Law Review 48

-- *Conflicts of Law and Morality* (Oxford University Press, New York 1989)

Greene S and O'Brien C O, 'Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct under the Computer Fraud and Abuse Act' (2013) 50 American Business Law Journal 1

Greenpeace 'Bhopal Protests Move Online' (*Greenpeace*, 10 March 2003) <http://www.greenpeace.org/international/en/news/features/bhopal-protests-move-online/> accessed 24 October 2010

Griffin J G H, 'The'secret Path'of Grokster and Corley: Avoiding Liability for Copyright Infringement' (2005) 10 Communications Law 147

Griffith M, *Sophocles: Antigone* (Cambridge University Press, Cambridge 1999)

Gross H, A *Theory of Criminal Justice* (Oxford University Press, Oxford 1979)

Gross S R et al., *Exonerations in the United States 1989-2003* (University of Michigan, 2004) <http://www.mindfully.org/Reform/2004/Prison-Exonerations-Gross19apr04.htm> accessed 15 August 2013

Grossman J, 'Social Backgrounds and Judicial Decision-Making' (1966) 79 Harvard Law Review 1551

H

Habermas J, 'Civil Disobedience: Litmus Test for the Democratic Constitutional State' (1985) 30 Berkeley Journal of Sociology 95

-- *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (William Rehg tr, Polity, Cambridge 1996)

Habermas J and Calhoun M, 'Right and Violence: A German Trauma' (1985) 1 Cultural Critique 125

Habib J, 'Cyber Crime and Punishment: Filtering out Internet Felons' (2003) 14 Fordham Intellectual Property Media & Entertainment Law Journal 1051

Hacktivismo 'cDc Releases Goolag Scanner' (*Hacktivismo*, 20 February 2008 <http://www.hacktivismo.com/news/ accessed 29/07/2010> accessed 22 December 2012

-- 'Hacktivismo Projects' (*Hacktivismo*, undated) <http://www.hacktivismo.com/projects/index.php> accessed 01 December 2012

-- 'About Hacktivismo' (*Hacktivismo,* undated) <http://www.hacktivismo.com/about/index.php> accessed 20 September 2011

Haksar V, 'Civil Disobedience and Non-Cooperation' in Bedau H (ed), *Civil Disobedience in Focus* (Routledge, London 2002)

-- 'The Right to Civil Disobedience' (2003) 41 Osgoode Hall Law Journal

Hall R, 'Legal Toleration of Civil Disobedience' (1971) 81 Ethics 128

Halliday J, 'Anonymous Hackers Jailed for Cyber Attacks' (*The Guardian*, 24 January 2013) <http://www.guardian.co.uk/technology/2013/jan/24/anonymous-hackers-jailed-cyber-attacks> accessed 18 June 2013

Hampson N, 'Hacktivism: A New Breed of Protest in a Networked World' (2012) 35 Boston College International & Comparative Law Review 511

Hampton J, 'The Moral Education Theory of Punishment' (1984) 13 Philosophy & Public Affairs 208

Haney C 'The Psychological Impact of Incarceration: Implications for Postprison Adjustment' in Travis J and Waul M (eds), *Prisoners Once Removed: The Impact of Incarceration and Reentry on Children, Families, and Communities* (Urban Institute Press 2003)

Hardt M and Negri A, *Empire* (4th edn, Harvard University Press, Cambridge (Ma) 2001)

Hart H L A, 'Are There Any Natural Rights?' (1955) 64 The Philosophical Review 175

-- *Punishment and Responsibility: Essays in the Philosophy of Law* (Oxford University Press, Oxford 1968)

Herring J, *Criminal Law* (3rd edn, Palgrave Macmillan, Hampshire 2002)

Herwig J 'Anonymous: Peering behind the Mask' (*The Guardian,* 11 May 2011) <http://www.guardian.co.uk/technology/2011/may/11/anonymous-behind-the-mask> accessed 21 September 2011

Heymann L, 'Inducement as Contributory Copyright Infringement: Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd' (2006) 37 International Review of Intellectual Property and Competition Law 31

Himma K E (2005) 'Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?' <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=799545#> accessed 19 June 2013

Hintz A, 'Deconstructing Multi-Stakeholderism: The Discourses and Realities of Global Governance at the World Summit on the Information Society (WSIS)' (Central European University, Budapest 2007)

Hintz A and Milan S, 'At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy' (2009) 5 International Journal of Media & Cultural Politics 23

Hobbes T, *Leviathan* (1651) <http://oregonstate.edu/instruct/phl302/texts/hobbes/leviathan-contents.html> accessed 20 June 2013

Holland B, 'The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty (Draft)' (2005) 24 Journal of Computer and Information Law

Holloway W and Jefferson T, 'The Risk Society in an Age of Anxiety: Situating Fear of Crime' (1997) 48 The British Journal of Sociology 255

Holmes Jr O W, *The Common Law* (Paulo J. S. Pereira and Diego M. Beltran (eds), University of Toronto Law School Typographical Society, Toronto 2011)

Home Office 'Electronic Monitoring on Bail for Adults - Procedures' (Home Office Circular 25, London 2006)

Honderich T, *Punishment: The Supposed Justifications Revisited* (Pluto Press, London 2006)

Honig B, 'Rawls on Politics and Punishment' (1993) 46 Political Research Quarterly 99

Hough M and Roberts J V, 'Sentencing Trends in Britain: Public Knowledge and Public Opinion' (1999) 1 Punishment & Society 11

House of Lords Select Committee on Science and Technology, 'Science and Technology - Fifth Report' (London, 2007) <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm> accessed 20 May 2013

Hudson B, *Justice in the Risk Society: Challenging and Re-Affirming Justice in Late Modernity* (Sage Publications Ltd, London 2003)

Husak D N, *Overcriminalization: The Limits of the Criminal Law* (Oxford University Press, Oxford 2008)

Hyne D, 'Examining the Legal Challenges to the Restriction of Computer Access as a Term of Probation or Supervised Release' (2002) 28 New England Journal on Criminal & Civil Confinement 215

I

International Telecommunication Union ICT Applications and Cybersecurity Division,'Understanding Cybercrime: A Guide for Developing Countries' (*International Telecommunication Union*, 2009) <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf> accessed 26 January 2013

J

Jansen R S, 'Populist Mobilization: A New Theoretical Approach to Populism' (2011) 29 Sociological Theory 75

Jarrett M, et al. 'Prosecuting Computer Crimes' (Criminal Division Computer Crime and Intellectual Property Section Criminal Division, Department of Justice, Washington D.C. undated) <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf> accessed 20 May 2011

Johnson B and Youm H, 'Commercial Speech and Free Expression: The United States and Europe Compared' (2008) 2 Journal of International Media & Entertainement Law 159

Johnson D and Post D, 'Law and Borders-the Rise of Law in Cyberspace' (1995) 48 Stanford Law Review 1367

Jordan T, *Activism!: Direct Action, Hacktivism and the Future of Society* (Reaktion Books, London 2002)

-- *Hacking: Digital Media and Technological Determinism* (Polity, Cambridge 2008)

Jordan T and Taylor P A, *Hacktivism and Cyberwars: Rebels with a Cause?* (Routledge, London 2004)

Juergen Habermas and Martha Calhoun, 'Right and Violence: A German Trauma' (1985) 1 Cultural Critique 125

Juris J S 'Networked Social Movements: Global Movements for Global Justice', in Castells M (ed), *The Network Society: A Cross-Cultural Perspective* (Edward Elgar Publishing Ltd, Cheltenham 2004)

K

Kahn D, 'Social Intermediaries: Creating a More Responsible Web through Portable Identity, Cross-Web Reputation, and Code-Backed Norms' (2010) 11 Columbia Science & Technology Law Review 176

Karagiannopoulos V, 'The Role of the Internet in Political Struggles: Some Conclusions from Iran and Egypt' (2012) 34 New Political Science 151

-- 'China and the Internet: Expanding on Lessig’s Regulation Nightmares' (2012) 9 SCRIPTed 150

Karnow C, 'Launch on Warning: Aggressive Defense of Computer Systems' (2004) 7 Yale Journal of Law & Technology 87

Katz B J, 'Civil Disobedience and the First Amendment' (1985) 32 UCLA Law Review 904

Kavada A, (2009) 'The Internet and Decentralized Architectures' in Karatzogianni A (ed), *Cyberconflicts and Global Politics* (Routledge, London 2009)

Kellner M M, 'Democracy and Civil Disobedience' (1975) 37 The Journal of Politics 899

Kelly M G E,*The Political Philosophy of Michel Foucault* (Taylor & Francis e-Library, 2009)

Kemshall H, *Understanding Risk in Criminal Justice* (Mike McGuire ed, Open University Press, Maidenhead 2003)

Kendrick K, 'The Tipping Point: Prison Overcrowding Nationally, in West Virginia, and Recommendations for Reform' (2011) 113 West Virginia Law Review 585

Kerr O S, 'Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes' (2003) 78 New York University Law Review 1596

-- 'Vagueness Challenges to the Computer Fraud and Abuse Act' (2010) 94 Minnessota Law Review

Kesan J P and Rajiv S C, ‘Deconstructing Code’ (2003-4) 6 Yale Journal of Law & Technology 277

Kesan J P and Majuca R, 'Optimal Hackback' (2010) 84 Chicago-Kent Law Review 831

Kahn D, 'Social Intermediaries: Creating a More Responsible Web through Portable Identity, Cross-Web Reputation, and Code-Backed Norms' (2010) 11 Columbia Science & Technology Law Review 176

Kierkegaard S M, 'Here Comes the 'Cybernators'!' (2006) 22 Computer Law & Security Report 381

Kiss J 'The Pirate Bay Trial: Guilty Verdict' (*The Guardian,* 17 April 2009) <http://www.guardian.co.uk/technology/2009/apr/17/the-pirate-bay-trial-guilty-verdict>, accessed 22 January 2013

Kizza J M, *Ethical and Social Issues in the Information Age* (Springer-Verlag, New York 2010)

Klang M, 'A Critical Look at the Regulation of Computer Viruses' (2003) 11 International Journal of Law and Information Technology 162

-- 'Civil Disobedience Online' (2004) 2 Info, Communications and Ethics in Society 75

-- 'Disruptive Technology: Effects of Technology Regulation on Democracy' (DPhil, Goeteborg University 2006)

Klein N, *No Logo: Taking Aim at the Brand Bullies* (Flamingo, London 2001)

-- *The Shock Doctrine* (Penguin Books, London 2007)

Kleinig J, *Ethics and Criminal Justice: An Introduction* (Cambridge University Press, Cambridge 2008)

Knafo S 'Occupy Wall Street and Anonymous: Turning a Fledgling Movement into a Meme' (huffingtonpost.com, 20 October 2011) <http://www.huffingtonpost.com/2011/10/20/occupy-wall-street-anonymous-connection_n_1021665.html> accessed 01 December 2012

Knappenberger B, 'We Are Legion: The Story of the Hacktivists', (*YouTube*, 19 June 2013) <https://www.youtube.com/watch?v=ELcAEwJdTeQ> accessed 02 August 2013

Koops B-J 'Criteria for Normative Technology: The Acceptability of ‘Code as Law’ in Light of Democratic and Constitutional Values' in Brownsword R and Yeung K (eds), *Regulating Technologies Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008)

Kramer M and Lombardi F, 'New Top State Judge: Abolish Grand Juries & Let Us Decide' (*New York Daily News,* New York 1985)

Krauss R, 'The Theory of Prosecutorial Discretion in Federal Law: Origins and Developments' (2009) 6 Seton Hall Circuit Review 1

Kravets D 'Virtual Sit-Ins Doom Online Animal Rights Activists' (*ThreatLevel Blog*, 16 October 2009) <http://www.wired.com/threatlevel/2009/10/animals/> accessed 20 May 2011

-- 'Guilty Plea in 'Anonymous' DDoS Scientology Attack' (*ThreatLevel Blog,* 26 January 2010) <http://www.wired.com/threatlevel/2010/01/guilty-plea-in-scientology-ddos-attack/> accessed 20 May 2011

-- 'Analysis: FCC Comcast Order is Open Invitation to Internet Filtering' (*Threat Level Blog,* 20 August 2012) <http://www.wired.com/threatlevel/2008/08/analysis-fcc-co/> accessed 23 June 2013

Krygier M, 'Ethical Positivism and the Liberalism of Fear' (1999) 24 Australian Journal of Legal Philosophy 65

Kumar M, 'Anonymous Hit Egyptian Government Websites as #Opegypt' (*The Hacker News*, 09 December 2012)

L

La Rue F, '*Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Vi. Conclusions and Recommendations'* (United Nations General Assembly, 16 May 2011)<http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf> accessed 14 February 2013

Ladeur K-H, 'Prozedurale Rationalitaet – Steigerung der Legitimationsfaehigkeit oder der Leistungfaehigkeit des Rechtssystems?' 7 Zeitschrift fuer Rechtssoziologie 265

Lambek B D, 'Necessity and International Law: Arguments for the Legality of Civil Disobedience' (1987) 5 Yale Law & Policy Review 472

Lane J and Dominguez R, 'Digital Zapatistas' (2003) 47 TDR 129

Law Commission, 'Computer Misuse' (Hansard Report No.186, 1989)

Lazos G, *Informatics and Crime* (Nomiki Vivliothiki, Athens 2000)

Lee M, et al., 'Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal' (1999) 14 Berkeley Technology Law Journal 839

LeGrande J L, 'Nonviolent Civil Disobedience and Police Enforcement Policy' (1967) 58 The Journal of Criminal Law, Criminology, and Police Science 393

Lessig L, *Code and Other Laws of Cyberspace* (Basic Books, New York 1999)

-- *Code v.2.0* (Basic Books, New York 2006)

-- 'Prosecutor as Bully' (*Lessig Blog, v2*, 12 January 2013) <http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully> accessed 20 June 2013

Levy P A 'Responding to Prosecutors Seeking to Identify Anonymous Bloggers — Google and Other ISP's Could Learn from the Mainstream Media' (*Consumer Law and Policy Blog*, 17 November 2010) <http://pubcit.typepad.com/clpblog/2010/11/responding-to-prosecutors-seeking-to-identify-anonymous-bloggers-google-and-other-isps-could-learn-f.html> accessed 23 November 2012

Levy S, *Hackers: Heroes of the Computer Revolution* (Bantam Doubleday Dell, New York 1984)

Leyden J, 'Webroot Guesstimates Inflate UK Spyware Problem' (*The Register*, 20 October 2005) <http://www.theregister.co.uk/2005/10/20/webroot_uk_spyware_guesstimates/> accessed 21 April 2012

-- 'Techwatch Weathers DDoS Extortion Attacks' (*The Register,* 30 January 2009) <http://www.theregister.co.uk/2009/01/30/techwatch_ddos/> accessed 26 October 2010

-- 'Iranian Hacktivists Hand-Crank Ddos Attack' (*The Register,* 22 June 2009) <http://www.theregister.co.uk/2009/06/22/iranian_hactivism/> accessed 20 October 2010

-- 'Spanish Poice Cuff Three Anonymous Hack Suspects' (*The Register,* 10 June 2011) <http://www.theregister.co.uk/2011/06/10/spain_anonymous_arrests/> accessed 21 September 2011

-- 'Anonymous Unsheathes New, Potent Attack Weapon' (*The Register*, 04 August 2011) <http://www.theregister.co.uk/2011/08/04/anon_develops_loic_ddos_alternative/> accessed 11 September 2011.

Liedtke M, 'Google's Motorola Mobility Acquisition Closes' (*Huffington Post,* 22 May 2012) <http://www.huffingtonpost.com/2012/05/22/google-motorola-mobility-acquisition-closes_n_1535719.html?ref=technology> accessed 29 May 2012

Lievrouw L A, 'Oppositional and Activist New Media: Remediation, Reconfiguration, Participation' (*Proceedings of the Ninth Participatory Design Conference*, Trento 2006) http://www.itu.dk/people/kremer/200djs/artikler/p115-lievrouw.pdf accessed 03 August 2013

Lippman M, 'Civil Disobedience: The Dictates of Conscience Versus the Rule of Law' (1986) 26 Washburn Law Journal 233

Lippman M R, *Contemporary Criminal Law: Concepts, Cases, and Controversies* (Sage Publications, London 2010)

Lloyd I J, *Information Technology Law* (6th edn, Oxford University Press, Oxford 2011)

Loader I and Walker N, *Civilizing Security* (Cambridge University Press, Cambridge 2007)

Loesch M C, 'Motive Testimony and a Civil Disobedience Justification' (1990) 5 Notre Dame Journal of Law, Ethics & Public Policy 1069

Lofgren Z and Wyden R 'Introducing Aaron’s Law, a Desperately needed Reform of the Computer Fraud and Abuse Act’ (*Wired,* 20 June 2013) <http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here/> accessed 21 June 2013

Logan C C, 'Liberty or Safety: Implications of the USA Patriot Act and the UK's Anti-Terror Laws on Freedom of Expression and Free Exercise of Religion' (2006) 37 Seton Hall Law Review 863

Loren L P, 'Deterring Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously' (2011) 46 Wake Forest Law Review 745

Lovink G and Rossiter N, 'Dawn of the Organised Networks' (2005) 5 Fibreculture Journal <http://five.fibreculturejournal.org/fcj-029-dawn-of-the-organised-networks/> accessed 15 February 2013

Lucchi N, 'Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression' (2011) 19 Cardozo Journal of International and Comparative Law 646

Lupton D *Risk* (Taylor and Francis E-Library, 2005)

M

MacDonald M, Greifinger R, and Kane D, 'The Impact of Overcrowding' (2012) 8 International Journal of Prisoner Health

MacKinnon R, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, New York 2012)

Majone G 'Regulatory Legitimacy' in Richardson J (ed), *Regulating Europe* (Routledge, London 1996)

Malik S 'Cyber Crime 'Threatens UK Stockmarket, Pensions and Businesses'' (*The Guardian*, 02 March 2011) <http://www.guardian.co.uk/uk/2011/mar/02/cyber-crime-threat-uk> accessed 29 September 2011

Mann R and Belzley S, 'The Promise of Internet Intermediary Liability' (2005) 47 William & Mary Law Review 239

Mansfield-Devine S, 'Anonymous: Serious Threat or Mere Annoyance?' (2011) Network Security 4

Markovits D, 'Democratic Disobedience' (2005) 114 The Yale Law Journal 1897

Masnick M 'Why Didn't Google or Comcast Protect the Identity of Anonymous Church Blogger Who Was Outed?' (*Techdirt*, 18 November 2010) <http://www.techdirt.com/articles/20101118/05102511923/why-didn-t-google-or-comcast-protect-the-identity-of-anonymous-church-blogger-who-was-outed.shtml> accessed 02 September 2012

McCullagh D 'Renewed Push to Give Obama an Internet "Kill Switch"' (*TechTalk*, 24 January 2011) <http://www.cbsnews.com/8301-501465_162-20029302-501465.html> accessed 01 June 2012

McGuire M, *Hypercrime: The New Geometry of Harm* (Routledge Cavendish, Oxford 2007)

McIntyre TJ and Scott C 'Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility' in Brownsword R and Yeung K (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008)

McLeod I, *Legal Theory* (2nd edn, Palgrave MacMillan, New York 2003)

McNamee J, ‘The Slide from “Self-Regulation” to Corporate Censorship’ (*European Digital Rights,* Brussels 2011) <http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf> accessed 15 February 2013

Mead D, *The New Law of Peaceful Protest: Rights and Regulation in the Human Rights Act Era* (Hart Publishing, Oxford 2010)

Meikle G 'Electronic Civil Disobedience and Symbolic Power' in Karatzogianni A (ed), *Cyberconflicts and Global Politics* (Routledge, London 2009)

Melilli K J, 'Prosecutorial Discretion in an Adversary System' (1992) Brigham Youth University Law Review 669

Mezzofiore G, 'Anonymous Targets Facebook, IBM, Intel and AT&T in Operation Defense Phase II' *(IBTimes*, 13 April 2012) <http://www.ibtimes.co.uk/articles/327682/20120413/cispa-operation-defense-anonymous-pledges-attack-intel.htm> accessed 21 June 2013

Mill J S, *Utilitarianism* (Original Edition 1879, The Floating Press 2009)

Mills E, 'Wikileaks Fans Should Think before They Botnet' (*CNet,* 10 December 2010) <http://news.cnet.com/8301-27080_3-20025373-245.html> accessed 28 September 2011

-- 'Anonymous to Target Iran with Dos Attack' (*CNet,* 29 April 2011) <http://news.cnet.com/8301-27080_3-20058700-245.html> accessed 21 June 2013

-- 'Anonymous Exposes Info of Alleged Pepper Spray Cop' (*CNet,* 26 September 2011) <http://news.cnet.com/8301-27080_3-20111813-245/anonymous-exposes-info-of-alleged-pepper-spray-cop/> accessed 15 August 2012.

Mills S, *Foucault* (Routledge, London 2003)

Milone M G, 'Hactivism: Securing the National Infrastructure' (2002) 58 The Business Lawyer 383

Mintz, H, ''Anonymous' Defendants Appear in San Jose Federal Court in Paypal Cyberattack Case' (*Mercury News,* 01 September 2011) <http://sip-trunking.tmcnet.com/news/2011/09/01/5747845.htm> accessed 01 September 2011

Mib, 'cDc Releases Goolag Scanner' (*Hacktivismo,* 20 February 2008) <http://www.hacktivismo.com/news/> accessed 20 September 2011

Moitra S D, 'Developing Policies for Cybercrime-Some Empirical Issues' (2005) 13 European Journal of Crime, Criminal Law & Criminal Justice 435

Morgan B and Yeung K, *An Introduction to Law and Regulation: Text and Materials* (Cambridge University Press, Cambridge 2007)

Morozov E 'In Defense of DDoS' (*Slate Magazine*, 13 December 2010) <http://www.slate.com/id/2277786/> accessed 20 May 2011

-- *The Net Delusion: The Dark Side of Internet Freedom* (*Public Affairs,* New York 2011)

Morreal J 'The Justifiability of Violent Civil Disobedience' in Bedau H (ed), *Civil Disobedience in Focus* (Routledge, London 1976)

Mueller M, Mathiason J and Klein H, 'The Internet and Global Governance Principles and Norms for a New Regime' (2007) 13 Global Governance 237

Murray A D, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge, London 2007)

Musiani F 'The Internet Bill of Rights Project: The Challenge of Reconciliation between Natural Freedoms and Needs for Regulation' (Fourth Annual GigaNet Symposium, Sharm-el-Sheikh, Egypt, 2009)

Myers H, 'Anonymous Anarchist Action Hacktivist Group Founded' (*libcom.org,* 10 March 2011) <http://libcom.org/news/anonymous-anarchist-action-hacktivist-group-founded-10032011> accessed 22 September 2011

N

Netanel N W, 'Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory' (2000) 88 California Law Review 395

Newman A 'Hacker Group Takes on Fed, IMF, "Global Banking Cartel"' (*The New American*, 15 March 2011) <http://www.thenewamerican.com/tech/computers/item/7213-hacker-group-takes-on-fed-imf-global-banking-cartel> accessed 12 August 2011

Nicolson D and Webb J S, *Professional Legal Ethics: Critical Interrogations* (Oxford University Press, Oxford 1999)

Nicolson D, 'Ideology and the South African Judicial Process-Lessons from the Past' (1992) 8 South Africa Journal on Human Rights 50

Noga K E, 'Securitizing Copyrights: An Answer to the Sonny Bono Copyright Term Extension Act' (2007) 9 Tulane Journal of Technology & Intellectual Property 1

Norrie A, *Crime, Reason and History: A Critical Introduction to Criminal Law* (Butterworths Tolley, London 2001)

Nunziato D C, 'The Death of the Public Forum in Cyberspace' (2005) 20 Berkeley Technology Law Journal 1115

O

O'Neill F J, 'Symbolic Speech' (1975) 43 Fordham Law Review 590

Ohm P, 'The Myth of the Superuser: Fear, Risk, and Harm Online' (2008) 41 University of California Davis Law Review 1327

Oliver P E, 'Bringing the Crowd Back In: The Non-organizational Elements of Social Movements' (1989) 11 Research in Social Movements, Conflict and Change 1

On the Media 'Defending Hacktivism' (*On the Media*, 17 December 2010) <http://www.onthemedia.org/transcripts/2010/12/17/02> accessed 20 May 2011

Organisation for Economic Co-Operation and Development (OECD), *The Economic and Social Role of Internet Intermediaries* (*OECD*, 2010)< http://www.oecd.org/internet/ieconomy/44949023.pdf> accessed 23 February 2013

Out-Law, 'UK Law Makes Hacking an Act of Terrorism' (*Out-Law,* 21 February 2001) <http://www.out-law.com/default.aspx?page=1409> accessed 20 May 2011

-- 'Commission Proposes New EU Cybercrime Law' (*The Register*, 11 October 2010) <http://www.theregister.co.uk/2010/10/11/eu_new_cybercrime_law/print.html> accessed 10 November 2012

P

Packer H L, *The Limits of the Criminal Sanction* (Stanford University Press, Stanford 1968)

Page B I and Shapiro R Y, 'Effects of Public Opinion on Policy' (1983) 77 The American Political Science Review 175

Palfrey J, 'Four Phases of Internet Regulation' (The Berkman Center for Internet & Society, Research Publication Series 2009-10) <http://cyber.law.harvard.edu/publications> accessed 18 December 2012

Parker C, *Just Lawyers: Regulation and Access to Justice* (Oxford University Press, Oxford 1999)

Parnell B-A 'Brit Mastermind of Anonymous Paypal Attack Gets 18 Months' Porridge' (*The Register,* 24 January 2013) <http://www.theregister.co.uk/2013/01/24/uk_anonymous_hackers_sentencing_payback/> accessed 26 January 2013

Pasquale F 'Trusting (and Verifying) Online Intermediaries' Policing' in Szoka B and Marcus A (eds), *The Next Digital Decade: Essays on the Future of the Internet* (Techfreedom, Washington D.C. 2010)

PayPal 'Update on Paypal Site Status' (*The PayPal Blog,* 09 December 2010) <https://www.thepaypalblog.com/2010/12/update-on-paypal-site-status/> accessed 09 September 2012

Perritt Jr H H, 'Towards a Hybrid Regulatory Scheme for the Internet' (2001)The University of Chicago Legal Forum 215

Philips M, 'The Justification of Punishment and the Justification of Political Authority' (1986) 5 Law and Philosophy 393

Pickerill J, 'Radical Politics on the Net' (2006) 59 Parliamentary Affairs 266

Pickett B L, 'Foucault and the Politics of Resistance' (1996) 28 Polity 445

Podgor E S, 'Cybercrime: Discretionary Jurisdiction' (2009) 47 University of Louisville Law Review 727

Posner R A, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (Oxford University Press, Oxford 2006)

Post D (1995) 'Anarchy, State and the Internet' 3 Journal of Online Law <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=943456> accessed 18 December 2012

Poullet Y, 'How to Regulate Internet: New Paradigms for Internet Governance Self-Regulation: Value and Limits' (2001) 20 Cahiers du Centre de Recherches Informatique et Droit 79

Power P F, 'Civil Disobedience as Functional Opposition' (1972) 34 The Journal of Politics 37

Q

Quint P E, *Civil Disobedience and the German Courts: The Pershing Missile Protests in Comparative Perspective* (Taylor and Francis e-Library, 2007)

R

Raghavan T M, 'In Fear of Cyberterrorism: An Analysis of the Congressional Response' (2003) Journal of Law Technology & Policy 297

Raley R, *Tactical Media* (University Of Minnesota Press, Minneapolis 2009)

Ranum M J, *The Myth of Homeland Security* (Wiley Publishing Inc, Indiana 2004)

Rawlinson K, 'Inside Anonymous: The "Hacktivists" in Their Own Words' (*The Independent,* 21 September 2011) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/inside-anonymous-the-quothacktivistsquot-in-their-own-words-2294935.html> accessed 21 September 2011

-- 'Activists Warned to Watch What They Say as Social Media Monitoring Becomes “Next Big Thing in Law Enforcement”' (*The Independent*, 01 October 2012) <http://www.independent.co.uk/news/uk/crime/activists-warned-to-watch-what-they-say-as-social-media-monitoring-becomes-next-big-thing-in-law-enforcement-8191977.html> accessed 06 October 2012.

Rawls J, 'Justice as Fairness: Political Not Metaphysical' (1985) 14 Philosophy and Public Affairs 223

-- *The Theory of Justice* (Harvard University Press, Cambridge 1999)

-- *The Law of the Peoples; with the Idea of Public Reason Revisited* (Harvard University Press, London 2000)

Raz J, *The Authority of Law: Essays on Law and Morality* (Oxford University Press, Oxford 1979)

Real D L and Honourable Irwin J F, 'Unconscious Influences on Judicial Decision-Making: The Illusion of Objectivity' (2010) 43 McGeorge Law Review

Reardon M 'Verizon Sued for Alleged Nsa Cooperation' (*CNet*, 15 May 2006) <http://news.cnet.com/Verizon-sued-for-alleged-NSA-cooperation/2100-1036_3-6072483.html> accessed 29 May 2012

Reed C, *Making Laws for Cyberspace* (Oxford University Press, Oxford 2012) 17-26

Reidenberg J R, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 Emory Law Journal 911

-- 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 Texas Law Review 533

-- 'States and Internet Enforcement' (2004) 1 University of Ottawa Law & Technology Journal 216

-- 'Technology and Internet Jurisdiction' (2004) 153 University of Pennsylvania Law Review 1951

Reynolds G, 'Ham Sandwich Nation: Due Process When Everything Is a Crime' (Legal Studies Research Paper No. 206, University of Tennessee 2013) <http://ssrn.com/abstract=2203713> accessed 20 June 2013

Rheingold H, *The Virtual Community: Homesteading on the Electronic Frontier* (The MIT Press, Cambridge (Ma) 2000)

Rietjens B, 'Give and Ye Shall Receive! The Copyright Implications of Bittorrent' (2005) 2 SCRIPT-ed 108

Roberts J V, 'Sentencing Guidelines and Judicial Discretion' (2011) 51 British Journal of Criminology 997

Roberts J V, and Hough M, 'Sentencing Riot-Related Offending: Where Do the Public Stand?' (2013) 53 British Journal of Criminology 1

Robinson P H, 'Why Does the Criminal Law Care What the Layperson Thinks Is Just? Coercive Versus Normative Crime Control' (2000) 86 Virginia Law Review 1839

Robinson P H and Dubber M D, 'An Introduction to the Model Penal Code' (2007) 10 New Criminal Law Review 319

Rosenzweig P, 'Overcriminalization: An Agenda for Change' (2004) 54 American University Law Review 809

Rousseau J-J, *The Social Contract* (The Penguin Group, London 2004)

Rozenberg J 'Buthurst Normal Reprimanded' (*Standpoint Magazine*, 07 October 2010) <http://standpointmag.co.uk/node/3462 > accessed 21 June 2013

Ruffin O, 'Hacktivism: From Here to There' (*cDc Communications,* 06 March 2004) <http://www.cultdeadcow.com/cDc_files/cDc-0384.html> accessed 20 September 2011

S

Salamon L (ed),*The Tools of Government: A Guide to the New Governance* (Oxford University Press, Oxford 2002).

Salter M and Mason J, *Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research* (Longman Publishing Group, London 2007)

Samuel A W (2004), 'Hacktivism and the Future of Political Participation' (DPhil Thesis, Harvard University 2004)

Sanchez M 'Bronx D.A. Withdraws Subpoena Seeking Identity of Anonymous Room Eight Posters' (*Citizen Media Law Project*, 17 July 2008) <http://www.citmedialaw.org/blog/2008/bronx-da-withdraws-subpoena-seeking-identity-anonymous-room-eight-posters> accessed 19 December 2012

Schesser S D, 'A New Domain for Public Speech: Opening Public Spaces Online' (2006) 94 California Law Review 1791

Schjølberg S, '*ITU Global Cybersecurity Agenda [GCA]*' (High Level Experts Group [HLEG] Global Strategic Report, International Telecommunications Union, Geneva 2008)< http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf> accessed 15 February 2013

Schlesinger S R, 'Civil Disobedience: The Problem of Selective Obedience to Law' (1976) 3 Hastings Constitutional Law Quarterly 947

Schopp R F, *Justification Defenses and Just Convictions* (Cambridge University Press, Cambridge 1998)

Schor E, 'Telecoms Granted Immunity in Us Wiretapping Probe' (*The Guardian,* 20 June 2008) <http://www.guardian.co.uk/world/2008/jun/20/georgebush.usa> accessed 21 June 2013

Schwarz A M, 'Civil Disobedience' (1970) 16 McGill Law Journal 542

Scott C, 'Accountability in the Regulatory State' (2000) 27 Journal of Law and Society 38

Segall L, 'Anonymous Strikes Back after Feds Shut Down Piracy Hub Megaupload' (*CNN Money,* 20 January 2012) <http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm> accessed 20 July 2013.

Seid R A, 'A Requiem for O'Brien: On the Nature of Symbolic Speech' (1992) 23 Cumberland Law Review 563

Sentencing Guidelines Council, 'Overarching Principles: Seriousness' (2004) <http://sentencingcouncil.judiciary.gov.uk/docs/web_seriousness_guideline.pdf> accessed 15 February 2013

Sentencing Guidelines Council, 'Magistrate's Court Sentencing Guidelines: Definitive Guideline' (2012) <http://sentencingcouncil.judiciary.gov.uk/docs/MCSG_Update9_October_2012.pdf> accessed 21 June 2013

Shane D, 'Think Tank Calls for 'Geneva Convention' on Cyber War' (*Information Age,* 04 February 2011) <http://www.information-age.com/technology/security/1599193/think-tank-calls-for-'geneva-convention'-on-cyber-war> accessed 10 November 2012

Shapiro I (ed), *Two Treatises of Government and a Letter Concerning Toleration* (Yale University Press, London 2003)

Shapiro M, *Who Guards the Guardians? Judicial Control of Administration* (University of Georgia Press, Athens 1988)

Shearing C and Wood J, 'Nodal Governance, Democracy, and the New 'Denizens'' (2003) 30 Journal of Law and Society 400

Shearing C, 'Reflections on the Refusal to Acknowledge Private Governments' in Jennifer Wood and Benoit Dupont (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge 2006) 11-32

Sherman L W, 'Defiance, Deterrence, and Irrelevance: A Theory of the Criminal Sanction' (1993) 30 Journal of Research in Crime and Delinquency 445

Shore M, Du Y, and Zeadally S, 'A Public-Private Partnership Model for National Cybersecurity' (2011) 3 Policy and Internet 1

Simon B 'Illegal Knowledge: Strategies for New Media Activism: Dialogue with Ricardo Dominguez and Geert Lovink' in Bousquet M and Wills K (eds), *The Politics of Information: The Electronic Mediation of Social Change* (Altx Press 2003)

Simon J, *Governing through Crime* (Oxford University Press, Oxford 2007)

Simmonds N E, *Central Issues in Jurisprudence* (3rd edn, Sweet and Maxwell Ltd, London 2008)

Singel R 'Dutch Arrest Teen for Pro-Wikileaks Attack on Visa and Mastercard Websites' (*Threat Level*, 09 December 2010) <http://www.wired.com/threatlevel/2010/12/wikileaks_anonymous_arrests/#seealsoaff033736dd3e21e1f35daab3a12f8f9> accessed 12 August 2011

Sinrod E and Reilly W, 'Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws' (2000) 16 Santa Clara Computer & High Tech Law Journal 177

Skibell R, 'Cybercrime and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act' (2003) 18 Berkeley Technogy Law Journal 909

Smith B P, 'Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help' (2005) 1 Journal of Law Economy & Policy 171

Smith G and Reilly R J, 'Alleged 'Paypal 14' Hackers Seek Deal to Stay out of Prison after Nearly 2 Years in Limbo' (*Huffington Post,* 18 May 2013) <http://www.huffingtonpost.com/2013/05/18/paypal-14-hackers_n_3281768.html> accessed 20 May 2013

Smith M B E, 'Is There a Prima Facie Obligation to Obey the Law?' (1973) 82 The Yale Law Journal 950

Smith W, 'Civil Disobedience and Social Power: Reflections on Habermas' (2008) 7 Contemporary Political Theory 72

Somaiya R 'Activists Say Web Assault for Assange Is Expanding' (*New York Times*, 10 December 2010) <http://www.nytimes.com/2010/12/11/world/europe/11anonymous.html?_r=4> accessed 16 Januray 2010.

Sommer P, 'Criminalising Hacking Tools' (2006) 3 Digital Investigation 68

Sophos 'Security Threat Report 2012' (*Sophos,* 2012) <http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/html-03.aspx> accessed 30 August 2012

Stalbaum B 'Why I Made a Formal Statement to the UCSD Police' (*Walking Tools,* 21 July 2010) <http://www.walkingtools.net/?p=489> accessed 26 October 2010

Stein A R, 'Parochialism and Pluralism in Cyberspace Regulation' (2004) 153 University of Pennsylvania Law Review 2003

Storing H J 'The Case against Civil Disobedience' in Bedau H A (ed), *Civil Disobedience in Focus* (Routledge, London 2002)

Strong E W, 'Justification of Juridical Punishment' (1969) 79 Ethics 187

Sunstein C R, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge University Press, Cambridge 2005)

Sunstein C R, *Republic.Com 2.0* (Princeton University Press, Princeton 2007)

Swire P, 'No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime' (2009) 7 Journal on Telecommunications & High Technology Law 107

T

Tang L and Yang P, 'Symbolic Power and the Internet: The Power of a 'Horse'' (2011) 33 Media Culture Society 675

Taylor P A, *Hackers: Crime in the Digital Sublime* (Routledge, London 1999)

Techdirt 'The Internet Strikes Back: Anonymous Takes Down Doj.Gov, RIAA, MPAA Sites to Protest Megaupload Seizure' (*Techdirt,* 19 January 2012) <http://www.techdirt.com/articles/20120119/14494917475/internet-strikes-back-anonymous-takes-down-dojgov-riaa-mpaa-sites-to-protest-megaupload-seizure.shtml>, accessed 19 November 2012

Terban S, 'Anonymous and Their Alleged Propagandist Barrett Brown' (*Infosec Island,* 10 March 2011) <https://www.infosecisland.com/blogview/12441-Anonymous-and-Their-Alleged-Propagandist-Barrett-Brown.html> accessed 28 September 2011

Terranova T, *Network Culture: Politics for the Information Age* (Pluto Press, London 2004)

Teubner G, 'Juridification: Concepts, Aspects, Limits, Solutions' in Teubner G (ed), *Juridification of Social Spheres: A Comparative Analysis in the Areas of Labour, Corporate, Antitrust and Social Welfare Law* (De Gruyter, Berlin 1987)

-- *Law as an Autopoietic System* (Blackwell, Oxford 1993)

The Economist, 'Cyberwar: War in the Fifth Domain' (The Economist, July 3rd 2010) 25-27

The Electrohippies Collective, 'Cyberlaw UK: Civil Rights and Protest on the Internet' *(iwar.org,* 2000) <http://www.iwar.org.uk/hackers/resources/electrohippies-collective/comm-2000-12.pdf> accessed 15 February 2013

The Smoking Gun, 'Judge Lifts Twitter Ban on "Anonymous" 14' (*The Smoking Gun*, 19 March 2012) <http://www.thesmokinggun.com/documents/judge-lifts-anonymous-twitter-ban-145792> accessed 30 August 2012

Thomassen L, 'Within the Limits of Deliberative Reason Alone: Habermas, Civil Disobedience and Constitutional Democracy' (2007) 6 European Journal of Political Theory 200

Thompson T, 'Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the White Hats under the CFAA' (2008) 36 Florida State University Law Review 537

Tice M, 'Civil Disobedience: A Study of Law and Its Relation to Society' (1968) 13 South Dakota Law Review 356

Tiefenbrun S, 'Civil Disobedience and the US Constitution' (2003) 32 Southwestern University Law Review 677

Tierney T A, 'Civil Disobedience as the Lesser Evil' (1988) 59 University of Colorado Law Review 961

Tilley N (1995) 'Thinking About Crime Prevention Performance Indicators' in Laylock G (ed), *Police Research Group Crime Detection and Prevention Series* (Home Office Police Research Group, London 1995)

TorrentFreak 'Copyright Holders Punish Themselves with Crazy Dmca Takedowns' (*Torrentfreak*, 25 May 2012 <http://torrentfreak.com/copyright-holders-punish-themselves-with-crazy-dmca-takedowns-120525/> accessed 29 May 2012

Travis J and Waul M, *Prisoners Once Removed: The Impact of Incarceration and Reentry on Children, Families, and Communities* (Urban Institute Press, Washington D.C. 2003)

Tremlett G and Agencies In Istanbul, 'Turkish Arrests Intensify Global War between Hacker Activists and Police' (*The Guardian*, 13 June 2011) <http://www.guardian.co.uk/technology/2011/jun/13/turkish-arrests-global-war-hackers-police> accessed 21 September 2011

Trimegisto 'History of Anonymous Hacktivism' (*The Trembling Uterus Blog,* 26 January 2011) <http://tremblinguterus.blogspot.com/2011/01/history-of-anonymous-hacktivism.html> accessed 28 September 2011

Tunick M, 'Hegel on Justified Disobedience' (1998) 26 Political Theory 514

U

United States Department of Homeland Security, 'National Infrastructure Protection Plan: Information Technology Sector' (undated) <http://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-information-technology-snapshot-2011.pdf> accessed 30 August 2012

United States Department of Homeland Security, 'What Is Critical Infrastructure?' (undated) <http://www.dhs.gov/what-critical-infrastructure> accessed 20 June 2013

United States Department of Justice, 'United States Attorney's Manual' (1997) <http://www.justice.gov/usao/eousa/foia_reading_room/usam/> accessed 21 June 2013

United States Senate ‘The National Information Infrastructure Protection Act of 1995’ (1996) (Report 104-357)

United States Sentencing Commission, '2011 Federal Sentencing Guidelines Manual' (2011) <http://www.ussc.gov/Guidelines/2011_Guidelines/Manual_PDF/index.cfm> accessed 21 June 2013

Urbas G, 'Criminalising Computer Misconduct: Some Legal and Philosophical Concerns' (2006) 14 Asia Pacific Law Review 95

Urbelis A, 'Toward a More Equitable Prosecution of Cybercrime: Concerning Hackers, Criminals, and the National Security' (2004) 29 Vermont Law Review 975

V

Vamos N, 'Please Don’t Call It ‘Plea Bargaining’' (2009) 617 Criminal Law Review 617

van Kokswijk J 'Social Control in Online Society--Advantages of Self-Regulation on the Internet' (International Conference on Cyberworlds, Singapore 2010)

Vegh S 'Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank' in McCaughey M and Ayers M D (eds), *Cyberactivism: Online Activism in Theory and Practice* (Routledge, London 2003)

Verizon, '2011 Was the Year of the 'Hacktivist' According to the “Verizon 2012 Data Breach Investigations Report”' (*Verizon*, 2012) <http://newscenter.verizon.com/press-releases/verizon/2012/2011-was-the-year-of-the.html> accessed 10 November 2012

Vidanage H, 'Rivalry in Cyberspace and Virtual Contours of a New Conflict Zone: The Sri Lankan Case' in Karatzogianni A (ed), *Cyberconflicts and Global Politics* (Routledge, London 2009)

Vijayan J, ''Anonymous' Arrests Tied to Paypal DDoS Attacks, FBI Says' (*ComputerWorld*, 20 July 2011) <http://www.computerworld.com.au/article/394256/_anonymous_arrests_tied_paypal_ddos_attacks_fbi_says/> accessed 10 November 2012

Vikas S N, 'Anonymous' Operation India Removed from Facebook and Twitter' (*TheNextWeb*, 12 June 2011) <http://thenextweb.com/in/2011/06/12/anonymous-operation-india-removed-from-facebook-and-twitter/> accessed 30 August 2012

Violet Blue, 'Anonymous Attacks Child Porn Websites and Publish User Names' (*ZDnet Blog*, 21 October 2011) <http://www.zdnet.com/blog/violetblue/anonymous-attacks-child-porn-websites-and-publish-user-names/757> accessed 19 February 2012

Virilio P, *The Information Bomb* (Verso Books, New York 2005)

von Hirsch A, *Censure and Sanctions* (Oxford University Press, Oxford 1996)

-- 'Proportionate Sentences: A Desert Perspective' in Ashworth A and von Hirsch A (eds), *Principled Sentencing: Theory and Policy* (Oxford Hart Publishing 1998)

-- 'Seriousness and Severity' in von Hirsch A (ed), *Censure and Sanctions* (Oxford University Press, Oxford 2003)

von Hirsch A et al. (eds), *Restorative Justice and Criminal Justice: Competing or Reconcilable Paradigms?* (Hart Publishing, Oxford 2003)

W

Walden I, *Computer Crimes and Digital Investigations* (Oxford University Press, New York 2007)

Walker C, 'Cyber-Terrorism: Legal Principle and Law in the United Kingdom' (2005) 110 Penn State Law Review 625

-- 'Clamping Down on Terrorism in the United Kingdom' (2006) 4 Journal of International Criminal Justice 1137

Walker N, 'Legislating the Transcendental: Von Hirsch's Proportionality' (1992) 51 The Cambridge Law Journal 530

Walker I 'Interview: Naomi Klein' (*ABC*, 2001) <http://www.abc.net.au/tv/hacktivists/klein_int.htm> accessed 20 October 2010

Walker S, *Taming the System: The Control of Discretion in Criminal Justice, 1950-1990* (Oxford University Press, Oxford 1993)

Wall D, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, Cambridge 2007)

Walton R, 'The Computer Misuse Act' (2006) 11 Information Security Technical Report 39

Warner G 'Internet Anarchy: Anonymous Crowds Flex Their Muscles' (*CyberCrime and Doing Time Blog,* 13 December 2010) <http://garwarner.blogspot.com/2010/12/internet-anarchy-anonymous-crowds-flex.html> accessed 13 August 2011

Watkins M, Bradshaw T, and Menn J, 'Global Police Moves against ‘Hacktivists’' (The Financial Times*,* 27 January 2011) <http://www.ft.com/cms/s/0/db6f5ab0-2a34-11e0-b906-00144feab49a.html#axzz1YaNDtzCj> accessed 21 September 2011

Watts S, 'Former Lulzsec Hacker Jake Davis on His Motivations' (*BBC,* 16 May 2013) <http://www.bbc.co.uk/news/technology-22526021> accessed 18 May 2013

Webster F, *Theories of the Information Society* (3rd edn Routledge, London 2006)

West J L, ' Is Injustice Relevant? Narrative and Blameworthiness in Protester Trials' (Temple Law Review Forthcoming; Vermont Law School Research Paper No. 11-13, 2013) <http://ssrn.com/abstract=2247518> accessed 17 May 2013

Whitehead J W, 'Civil Disobedience and Operation Rescue: A Historical and Theoretical Analysis' (1991) 48 Washington & Lee Law Review 77

Wikipedia 'Netizen' <http://en.wikipedia.org/wiki/Netizen> accessed 25 June 2012

-- 'World Wide Web' <http://en.wikipedia.org/wiki/World_Wide_Web > accessed 29 May 2012.

-- 'List of Mergers and Acquisitions by Microsoft' <http://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Microsoft> accessed 29 May 2012

-- 'IP Address' <http://en.wikipedia.org/wiki/IP_address#cite_note-rfc760-0> accessed 29 May 2012

-- 'Mafiaboy' <http://en.wikipedia.org/wiki/MafiaBoy> accessed 11 March 2011

-- 'Internet Society (ISOC)' <http://en.wikipedia.org/wiki/Internet_Society> accessed 15 June 2012

-- 'Right to Internet Access' <http://en.wikipedia.org/wiki/Right_to_Internet_access> accessed 16 November 2011

Wilson C, 'Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress' (Library of Congress, Congressional Research Service, Washington D.C. 2008)

Winston S, '“Don’t Be Evil”: Uncovering the Implications of Google Search' (2011) 7 Dalhousie Journal of Interdisciplinary Management 1

Wittgenstein L, *Philosophical Investigations* (G.E.M. Anscombe, tr, 2nd ed, Blackwell, Oxford 1958

Wolff J, 'Interview: Howard Schmidt' (*MSNBC,* 21 December 2010) <http://www.newsweek.com/2010/12/21/interview-with-cyber-security-czar-howard-schmidt.html> accessed 18 January 2011

Wolff M A, 'Evidence-Based Judicial Discretion: Promoting Public Safety through State Sentencing Reform' (2008) 83 New York University Law Review 1389

Wood J, 'Research and Innovation in the Field of Security: A Nodal Governance View' in Wood J and Dupont B (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge 2006)

Wood J, Shearing C, and Froestad J, 'Restorative Justice and Nodal Governance' (2011) 35 International Journal of Comparative and Applied Criminal Justice 1

Woozley A D, 'Civil Disobedience and Punishment' (1976) 86 Ethics 323

Worley B 'Facebook: Another Privacy Scandal' (*ABCNews*, 19 October 2010 <http://abcnews.go.com/GMA/Consumer/facebook-privacy-scandal-facebooks-watergate/story?id=11912201#.T8dLoJLoU4k> accessed 31 May 2012.

Worthy J and Fanning M, 'Denial-of-Service: Plugging the Legal Loopholes?' (2007) 23 Computer Law & Security Report 194

Wright E O, *The Politics of Punishment: A Critical Analysis of Prisons in America* (National Criminal Justice Reference Service Library Collection Harper & Row Publishers, New York 1973)

Wu T (2003) 'When Code Isn't Law' 89 Virginian Law Review 103

Wu T and Yoo C, 'Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate' (2007) 59 Federal Communications Law Journal 575

Y

Yar M, *Cybercrime and Society* (Sage Publications Ltd, London 2006)

-- 'Public Perceptions and Public Opinion About Internet Crime' in Jewkes Y and Yar M (eds), *Handbook of Internet Crime* (Willand Publishing, Devon 2010)

Yeung K 'Towards an Understanding of Regulation by Design' in Brownsword R and Yeung K (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, Oxford 2008)

Z

Zandt D 'Are the Cyber Battles with the Enemies of Wikileaks the New Civil Disobedience?' (*Alternet*, 13 December 2010)

<http://www.alternet.org/story/149183/are_the_cyber_battles_with_the_enemies_of_wikileaks_the_new_civil_disobedience> accessed 28 September 2011

Zavrsnik A, 'Cybercrime Definitional Challenges and Criminological Particularities' (2008) 2 Masaryk University Journal of Law & Technology 1

Zedner L, 'Too Much Security?' (2003) 31 International Journal of the Sociology of Law 155

-- *Criminal Justice* (Oxford University Press, Oxford 2004)

-- 'Securing Liberty in the Face of Terror: Reflections from Criminal Justice' (2005) 32 Journal of Law and Society 507

-- 'Pre-Crime and Post-Criminology?' (2007) 11 Theoretical Criminology 261

-- *Security* (Routledge, New York 2009)

Zetter K 'Hackers Release 1 Million Apple Device IDs Allegedly Stolen from FBI Laptop' (*Wired*, 09 April 2012) <http://www.wired.com/threatlevel/2012/09/hackers-release-1-million-apple-device-ids-allegedly-stolen-from-fbi-laptop/> accessed 08 September 2012

Zhang C, 'Regulation of the Internet-New Laws and New Paradigms' (2006) 17 Journal of Law, Information & Science 53

Zittrain J, *The Future of the Internet and How to Stop It* (Yale University Press, Virginia 2008)

Zizek S 'Shoplifters of the World Unite' (*London Review of Books*, 19 August 2011) <http://www.lrb.co.uk/2011/08/19/slavoj-zizek/shoplifters-of-the-world-unite> accessed 24 August 2011

Zlotnick D M, 'The War within the War on Crime: The Congressional Assault on Judicial Sentencing Discretion' (2004) 57 South Methodist University Law Review 211

LIST OF ABBREVIATIONS

ACTA: Anti-Counterfeiting Trade Agreement

AT&T: American Telecom and Telegraph

CAE: Critical Art Ensemble

CD: Civil Disobedience

cDc: Cult of the Dead Cow

CFAA: Computer Fraud and Abuse Act

CIA: Central Intelligence Agency

CMA: Computer Misuse Act

DDOS: Distributed Denial of Service

DEA: Digital Economy Act

DPP: Director of Public Prosecutions

DRM: Digital Rights Management

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

ECD: Electronic Civil Disobedience

EDT: Electronic Disturbance Theater

EU: European Union

FBI: Federal Bureau of Investigations

FCC: Federal Communications Commission

HADOPI: Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet

HESSLA: Hacktivismo's Enhanced-Source Software License Agreement

ICANN: Internet Corporation for Assigned Names and Numbers

ICP: Internet Content Provider

IETF: Internet Engineering Task Force

IGF: Internet Governance Forum

IMF: International Monetary Fund

IP: Internet Protocol

iRC: Internet Relay Chat

IRS: Internal Revenue Service

ISOC: Internet Society

ISP: Internet Service Provider

IT: Information Technology

ITU: International Telecommunications Union

IWF: Internet Watch Foundation

LOIC: Low Orbit Ion Cannon

MPC: Model Penal Code

NGO: Non-Governmental Organisation

OS: Operating System

PET: Privacy-Enhancing Technologies

PJA: Police and Justice Act

SOPA: Stop Online Piracy Act

StGB: Strafgesetzbuch

TCP/IP: Transmission Control Protocol/Internet Protocol

UK: United Kingdom

URL: Universal Resource Locator

US: United States (of America)

USAPA: USA PATRIOT Act

WSIS: World Summit on the Information Society

WTO: World Trade Organisation

WWW: World Wide Web