

# Civil Disobedience Online

Mathias Klang

University of Göteborg, Göteborg, Sweden

Email: klang@informatik.gu.se

## ABSTRACT

*The Internet is used for every conceivable form of communication and it is therefore only natural that it should be used as an infrastructure even for protest and civil disobedience. The technology however brings with it the ability to carry out new forms of protest, in new environments and also involve changed consequences for those involved. This article looks at four criminal activities, which are used as active forms of Internet based protest in use today and analysis these forms in relation to the traditional civil disobedience discourse. The analysis is done by studying four basic criteria (disobedience, civil, non-violence and justification) found in tradition civil disobedience discourse and observing their applicability in online environments. The purpose of this article is to better understand the political protest activities carried out online and to see whether traditional civil disobedience theory embraces these new forms of political activism.*

### COVERAGE



## ONLINE DISOBEDIENCE

In its simplest form civil disobedience involves defying the law for a good cause. It is therefore essentially a conflict between the law and the individual's morality. The purpose of this article is to look at the use of civil disobedience in online environments to understand what civil disobedience is and if it can be implemented as a political force in the online domain. It is not the purpose of this article to attempt to explain the substantive legislation regulating each of the illegal activities. However it is important to describe the acts which we intend to discuss from the point of view of the legislator. The purpose of this is to give a brief introduction to the activity and its conflict with the legal regime. While there is a growing consensus in online criminal law this article maintains a mainly European Union and United Kingdom focus.

## Unsolicited email

The European discussion on this issue has been confused with different countries attempting to implement different methods to resolve the problem of unsolicited mail or, as it is popularly known, spam. AOL (2003) summarised spam for 2003 as unsolicited email containing mainly "Dubious education offers, pharmaceuticals, body enhancing hormones, and shady finance-related offers" the growth of spam has led to European legislative initiatives. A large part of any political activity is the ability to spread the political message. A natural first stage has been the creation of a web site with information; email has been used to create interest in the political message and to notify people of current events and actions. This use of email has however recently been made illegal within the European Union through the *Directive*

## KEYWORDS

Civil  
Disobedience  
  
Hacking  
  
Webpage  
Defacement  
  
Denial of  
Service  
  
Email Bombing

(2002/58/EC) on *privacy and electronic communications* which has been implemented in the United Kingdom through *The Privacy and Electronic Communications (EC Directive) Regulations*. This regulation criminalises “the transmission of unsolicited communications by means of electronic mail to individual subscribers...a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail...” (Article 22).

---

**The Guidance explains that the term direct marketing covers “a wide range of activities which will apply not just to the offer for sale of goods or services”**

---

Due to the wording of this regulation it is interesting to ascertain whether a political protest message can fall under the definition of “communication for the purposes of direct marketing”. The legal definition of direct marketing in the United Kingdom can be found in the Information Commissioners Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003 – Part 1: Marketing by Electronic Means which begins by stating that the *Data Protection Act* (DPA) defines direct marketing as “the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.” The Guidance explains that the term *direct marketing* covers “a wide range of activities which will apply not just to the offer for sale of goods or services, but also to the promotion of an organisation’s aims and ideals. This would include a charity or a political party making an appeal for funds or support and, for example, an organisation whose campaign is designed to encourage individuals to write to their MP [Member of Parliament] on a particular matter or to attend a public meeting or rally.” This definition therefore covers any use by an organisation wishing to market either their ideas or any direct actions which they are planning to undertake to any individuals who have not, in advance, accepted that they are prepared to receive email from the organisation.

## Email bombing

A number of organisations encourage members and the public to email messages of protest to key individuals. In certain cases all that is provided is the email address and a suggested text which can be copied into the body of the email. In other cases the system is automated that all an interested protester need do is to click on an icon. Examples of organisations which use these methods are Amnesty International (Urgent Action network),<sup>1</sup> Greenpeace (Cyberactivist Community),<sup>2</sup> CorpWatch,<sup>3</sup> Friends of the Earth,<sup>4</sup> American Anti-Slavery Group,<sup>5</sup> Oxfam NikeWatch,<sup>6</sup> Free Aung San Suu Kyi.<sup>7</sup>

Writing or encouraging others to write protest e-mail messages is a legitimate protest form that may however, in the United Kingdom, fall under section three of the Computer Misuse Act (CMA) if the intention of the mass emailing is to limit the legitimate users’ use of a computer system. However, even without this intent the process of email bombing is now a questionable act since it may also be criminalised by the same regulations for unsolicited email.

## Hacking

Originally a hacker was a term used for a good programmer but today this definition has been overshadowed by the definition of the hacker as a person who attempts to gain unauthorised access to a computer or computerised system and the information it contains. Following the outcome of *R v Gold*<sup>8</sup> the United Kingdom enacted the CMA to deal with hacking and other abuses computer technology.

The one sided media discourse surrounding hacking has been very much focused on the vulnerability involved in connecting an organisation to the Internet and on the dangers represented by hackers (Taylor, 1999). There is also a strong connection between the idea of the good or white-hat hacker, electronic civil disobedience and the development of hacktivism (Klang, 2004). However, while the act of hacking, or the gaining of illegal access, is in many cases both illegal (Klang, 2004) and not uncontroversial (Kerr, 2003) it is usually the means, and not the goal, of an act of civil

disobedience. This is not to say that those who carry out online civil disobedience are not considered to be hackers, by themselves or others (see for example NIPC 2001), but rather that the act of hacking is only part of the act of disobedience since it is a necessary component of webpage defacement.

### Webpage defacement

Webpage defacement entails gaining unauthorised access to a webpage and making modifications to the webpage. These modifications involve the addition of messages with or without the removal of the original data. Political webpage defacement can be carried out either to effect a political decision, such as an election. This was done in 1998 in Sweden, when on the eve of the Swedish general election the home page of the right wing opposition party was hacked. The page was altered and links to political and party information were replaced with links to pornography sites and to the left wing party. Defacement can also be carried out to protest government policy. This can be seen in the action carried out in April 2003, when the web page of the Irish Aviation Authority (<http://www.iaa.ie>) was hacked. The front page was replaced with the text containing the message “The people of Ireland demand that the Irish Government deny access to Shannon Airport to the U.S. military...The Irish people are told they live in a democratic, neutral country. Where is the democracy in the Irish government deciding without the vote of the people, that U.S. murderers have access to Shannon Airport?”<sup>9</sup> The hacker also included information that “Nothing has Been Deleted” therefore no information was lost by the Irish Aviation Authority.

Webpage defacements often tend to follow patterns of real world politics. Targets often follow areas of tension such as Pakistan and India or Israel and Palestine or individual events such as the bombing in Bali, which was followed by attacks from Indonesia and Malaysia against South Asian targets. Among the more notorious long term use of defacement as a political weapon are the actions of Indian and Pakistani hackers, their actions are motivated by the tensions in over the disputed

Kashmir territory. In his article Srijith (2002) studies over 700 documented Indian webpage defacements occurring during a period of 20 months. He points out that generally most defacement attacks peak after security flaws are announced but he also notes that the trends in India do not mirror this worldwide trend. According to Srijith the defacement in India is more politically motivated with the most prolific attackers of Indian web pages originating from Pakistan. This claim is further corroborated by the anti-Indian propaganda left on the defaced pages.

### Denial of service

The Denial of Service (DoS) attack is usually described as an incident which prevents a legitimate user or organisation from accessing a systems resource or the delaying of systems operations and functions. The incidents or attacks can be related to a specific network service such as email or to the domain name of the target. Attacking the domain name has the added advantage for the attacker that it tends to diminish all the victims online functions since the domain name cannot be resolved (Klang, 2004). These activities are criminalised by Section three of the CMA and Article 4 of the *Council Framework Decision on attacks against information systems*<sup>10</sup> which deals directly with the criminalisation of DoS attacks.

Traditionally the distributed denial of service attack entailed the coordination of traffic to a designated Web site. This coordination at first required the marshalling of many protesters to be prepared at their computers and to coordinate the sending of information at a given time and to a specific target. These attacks required a great deal of social cohesion and organisation amongst the protesters who sat alone in front of their computers in the virtual presence of others and accessed a web page repeatedly. These attacks are known as coordinated point-to-point DoS attacks and as can be imagined the coordination of an international effort for this type of protest was a complex affair since their success depends upon all the users attempting to access the target simultaneously (Klang, 2004).

Software has been developed to support these actions. The DoS software usually

helps the user by relieving the user from the tedium of having to repeatedly access and renew the connection to a web page. The first software to be developed to aid DoS was called FloodNet and was developed by the Electronic Disturbance Theatre. Today there are two basic forms of DoS attacks the client-side DoS, sometimes called the virtual sit-in, and the server-side DoS this article focuses on the client-side DoS. For a more detailed discussion on the technical differences and moral effects see Klang (2004).

---

**a public, non-violent political act contrary to law and carried out with the aim of bringing about change in law or policy**

---

### Summing up

It is interesting to note that many of the tactics used and discussed by online activists are illegal or are being criminalised. Additionally the *Convention on Cybercrime*<sup>11</sup> reinforces the legal position that these acts are criminal offences or should be criminalised. The Convention leaves very little room for interpretation in the acts of those who wish to use the methods mentioned above as tools of protest. It is interesting to note that while the trend is for criminalisation this does little to help those who have been effected by online acts of disobedience since they must still rely on civil cases to recoup damages.

## HISTORICAL DISOBEDIENCE

Disobedience is not a behaviour which is encouraged. Despite this, there are many situations where disobedience is praised as a virtue and obedience is punished. An example of the former in the American civil rights movement an example of the latter can be seen in the German attempts to come to terms with its history, several border guards have, since the fall of the Berlin Wall, been charged with manslaughter or attempted manslaughter for killings at the border. Our relationship to social

and legal rules is therefore not as clear and simple as we would like it to be. We praise the actions of those who have undertaken the classical acts of civil disobedience while we attempt to prevent, limit and punish those who would disobey today.

Civil disobedience can be simplistically defined as: disobeying the law in a good cause. The reason why this may be a simplistic definition is that the good cause is a very elusive. The political and philosophical traditions of disobedience arise from the actions of Thoreau's refusal to pay poll tax in protest of the federal government's war in Mexico, support of chattel slavery and the violation of the rights of the native Indians. His action was based on his perceived right and obligation to follow his conscience. Thoreau (1993) writes that he will "...not lend myself to the wrong which I condemn." While this refusal to be a party to wrongful acts may be an admirable trait; it is not an active attempt to stem injustice, rather a method of keeping ones own hands clean (Singer, 1973).

A more precise definition on civil disobedience has been formulated by Bedau (1961) who described it as a public, non-violent political act contrary to law and carried out with the aim of bringing about change in law or policy. Later Bedau (1970) would broaden his definition to refer to illegal acts, "committed openly...non-violently...and conscientiously...within the framework of the rule of law...with the intention of frustrating or protesting some law, policy or decision...of the government." While these definitions are an important basis for further discussion it is important to remember that definitions in this area are to a certain extent arbitrary and therefore it is not the role of the definition to control what disobedience is but rather form the basis for attempting to arrive at a consensus on what disobedience may be.

The developments of civil disobedience are strongly connected with both Tolstoy's (1884) writings on pacifist non-resistance (rather die than kill) and Gandhi's (1942) less ideologically clear but more proactive ahimsa (non-violence). In their most clear form the concepts of practical civil disobedience can be seen in the actions and writings of King. In his struggle we see the whole span of possible reactions to the law. From the strictest views that even unjust

laws are to be obeyed (Plato, 2002) to the moral obligation to reject immoral laws (King, 1963).

Therefore one can sum up the situation that there is an *a priori* obligation to obey the law. However, this rule may come into direct conflict with moral obligations and have the ability to cause more harm. Or the duty to obey may be overridden in certain cases by other more stringent obligations (Rawls, 1963). There are however objections (Suber, 1999) to this view these objections claim that there cannot be any form of civil disobedience in a democratic state since the injustice is created in a “just environment” and can therefore be changed by democratic means – thus removing any need for disobedience. Much of civil disobedience has been carried out in democratic environments there is no requirement that disobedience be carried out only in a non-democratic environment. Additionally the use of democratic channels to correct an unjust situation may in itself create a situation which perpetuates the injustice since there are, in theory, no limits to democratic means of action. In a democratic society a minority may be particularly burdened by legislation despite that the majority feels the situation to be equitable. It is important to make the distinction that while the state may be democratic; it does not necessary follow that all the practices therein are just. Singer (1973) has defined the process of disobedience as one method for a minority to appeal to the majority to reconsider an injustice. The need for disobedience in such an appeal is necessary when the democratic process itself prolongs the injustice. Disobedience is therefore not intolerance towards the system but view that the democratic process being allowed to run its course perpetuates the injustice. King (1963) goes further and states that there is an obligation to disobey in the situation where the law is unjust:

“For years now I have heard the word ‘Wait!’... We must come to see...that ‘justice too long delayed is justice denied.’...One may well ask, ‘How can you advocate breaking some laws and obeying others?’ The answer is found in the fact that there are two types of laws: just and unjust...One has not only a legal but a moral responsibility to obey just laws.

Conversely, one has a moral responsibility to disobey unjust laws.”

A final issue is the problem of how we can accept that disobedience of a certain group and not another? This type of argument is often referred to as the slippery slope. The idea being that we cannot allow any disobedience since the moment we accept any form of disobedience we will rapidly progress to the bottom of the slope and be required to accept all disobedience. Those who argue that the slippery slope will lead us to anarchy would prefer that no disobedience be allowed. This is a simple and elegant solution which provides us with an easily remembered rule. However the problem of disobedience is already complex attempting to simplify it with absolute rules is not an equitable solution. Using the slippery slope to create a feeling of insecurity is not an acceptable solution. Such arguments have been used and abused over a long period of time (Volokh, 2003) their complexity may create a desire to simplify let us not deny justice for the sake of simple arguments.

If we are to agree that there may be, in certain cases, morally justified disobedience then how shall these be motivated? To understand this we must look at four criteria: disobedience, civil, non-violence and justification. These criteria must be analysed and reinterpreted for application in the digital environment. These criteria have been chosen for their central role in discussions of disobedience but are not universally viewed as the only criteria worthy of discussion, see for example Fairweather’s (1999) discussion on seven criteria for identifying tolerable disobedience.

*Disobedience:* This is arguably the most important criteria since without this there is no discussion. A tolerance for disobedience is important in a civil society but to accept disobedience is not an option since disobedience by its nature, cannot be permitted. Disobedience stems from the conscious desire to protest a law which conflicts with “more stringent obligations” (Rawls, 1971). To comply, even with silent disapproval, does not constitute disobedience. To comply, after voicing disapproval, is laudable but not disobedience.

*Civil:* Disobedience brings with it unattrac-

tive consequences such as legal and social reactions and therefore there is a strong urge to hide ones disobedience. However it is important to remember that the publication of the disobedience is a necessary component of the actions and provide a greater degree of legitimacy (see for example King, 1963; Rawls, 1971; Singer, 1973). In situations where there is risk of great personal harm it is understandable that the disobedience does not take place publicly, however, civil disobedience generally has a role of public enlightenment (Bedau, 1991).

*Non-violence:* Due in part to its traditions, there is a misconception that equates civil disobedience with non-violent action. Violence on its own does not invalidate an action from being civil disobedience. However, it is important to note that the use of violence in civil disobedience has been shown to take the focus off the message of protest and creates a lack of sympathy towards those who use it. Violence is in itself not static and there are different levels of violence which may be implemented. Violence can be seen from the prevention of others enjoyment of their private property (such as the sit-in), the defacement or destruction of property across to the more extreme causing of bodily harm to others. In practice and in literature there is no acceptance, within the civil disobedience discourse, in the causing of physical harm to others. It is therefore important to remember that civil disobedience may necessitate a certain level of coercion or harm.

*Justification:* The classic justification of civil disobedience lies in a conflict of law with moral principle. Rawls (1971) is quite firm on this point, claiming that the protester must appeal to shared principles existing in the morality of the general public. Singer (1973) finds the qualification of shared values too limiting since the protester must appeal to a pre-existing norm. Another point of disagreement between Rawls and Singer is the question of the acceptance of punishment. While it naturally shows a great moral courage to be prepared to accept the punishment which stems from ones political acts – attempts to evade punishment on its own does not make the act less of civil disobedience.

## ONLINE CIVIL DISOBEDIENCE

It is interesting to note that the four criteria of civil disobedience discussed above have been developed in a pre-Internet environment and the question is whether they can be applied to disobedience in an online environment. If the criteria can be transferred into a digital environment then there is no reason why the use of digital technology as a form of protest should not be viewed as being functionally equivalent to other means of protest and be respected as such. If the four criteria do not transfer into the digital environment the question then becomes whether the online actions can be seen as legitimate forms of civil disobedience and therefore the theoretical basis of civil disobedience should be adjusted to fit the reality of the day. Alternatively the acts are merely illegal and have no moral justification as forms of protest.

*Disobedience:* Probably the easiest criterion to fulfil is the question of legality. The actions mentioned in this paper are illegal, or rapidly being criminalised in most jurisdictions. The act of criminalisation is taking place both in national legislation such as the CMA of the United Kingdom or the American Patriot Act and in regional developments such as EU directives and the Convention on Cybercrime. This move towards criminalisation has not only involved the loss of civil liberties in general but also brings with it an additional threat. This threat is the comparison of cyber crimes with terrorism which create a more serious environment for the perpetrator of such acts (Klang, 2004; Manion & Goodrum, 1999).

*Civil:* Online disobedience gives rise to many questions in relation to the term civil. Even if we accept that the actions are carried out to create publicity and to educate the general public it is interesting to note that online civil disobedience has been carried out in two untraditional circumstances. Firstly the attacks need not be directed only at state actors but even larger multinational corporations have been effected by disobedience. Secondly the disobedience is not only limited to citizens within the state they are protesting. These

circumstances have the effect that the actions fall outside the broader definition of civil disobedience put forward by Bedau (1970).

Taken together online disobedience offers the disobedient party the ability to carry out activities which hamper the lawful activities of a private actor in another country. This raises questions of legitimacy since the attacked party may be following the law and morality of the culture where business is carried out. Additionally those carrying out the disobedience are not personally effected by the action of the attacked party and therefore must rely on a secondary right. They are acting in the name of the injustice carried out against others. At first glance this may weaken the legitimacy of the disobedience.

*Non-violence:* The main complaint concerning violence in relation to online civil disobedience activities is in relation to the limitation of user's enjoyment of their property. In situations where webpage defacement, DoS attacks, mail bombing or unsolicited mail are used as tactics of civil disobedience they tend to impair the users (or the websites customers) legitimate use of property. Personal violence or physical harm can be caused if, for example, a user is dependent upon a website for information however, to this author's knowledge; no such cases have been reported. Damage to property in during these attacks is not necessary and even in the case of DoS attacks the web pages or services have been disrupted only for brief periods.

*Justification:* If we are to see justification as containing an acceptance of punishment (but not necessarily a masochistic search for one) and the active presentation of ones ideas, subjecting oneself to the evaluation of society, we can then evaluate these criteria by an example. *The electro hippie collective* use client-side DoS as a protest method and also maintains an open dialogue "...we do not try bury our identities from law enforcement authorities any authority could, if it chose to, track us down in a few hours. However, because some of us work in the IT industry, we do not make our general membership known because this would

endanger our livelihoods" (Electrohippies, 2000). They do not hide themselves or their actions but at the same time they do not advertise their identities. While the Rawlsian approach to disobedience may disapprove of their method, Singer (1973) seems to sympathise.

In terms of public education the group publishes its views on both their politics and their method of protest in a series of publications available freely online. This is an attempt to create a dialogue on the subject of the use of DoS as a political activism tool they have employed the sit-in as a metaphor and they term their attacks as virtual sit-ins. "Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure" (Electrohippies, 2000).

The electrohippies views are not unopposed, another group of activists argue that since DoS attacks are a violation of freedom of expression and assembly "No rationale, even in the service of the highest ideals, makes them anything other than what they are – illegal, unethical, and uncivil" (Ruffin, 2000). The electrohippies are aware of the paradox of using DoS attacks for the purpose of promoting open and free speech since they are curtailing the speech of others but they maintain that their actions are justified if the principles of proportionality, speech deficit, openness and accountability are adhered to.

---

**Our method has built within it the guarantee of democratic accountability**

---

Proportionality refers to the insight that it is not acceptable to disrupt communications without justification the attack itself must not be the focus. The tactic is a means and not an end, bringing publicity to an event which is the focus of the action. The action can only be legitimate if speech deficit exists i.e. a lack of equality between the actors within the public discourse. The attack must therefore be used to aw atten-

tion to this inequality and is not in itself the intended message. The principles of openness and accountability refer add to the legitimacy of the attack since without these it would be difficult to argue that the ultimate goal is an open discourse. In 2003 the electrohippies antiwar protest managed to disrupt the webpage of the Prime Minister (<http://www.number-10.gov.uk/>) causing it to be unavailable on several occasions. In response to criticism of their actions they argued that their actions do not prevent any communications between the allies but are intended to show the use of official websites as a part of the propaganda directed at “seeking to sanitise their violation of International human rights law. Action by the Collective is therefore valid in order to highlight their violation of fundamental rights by a method that seeks to restrict their misuse of the right to freedom of expression under the UN Universal Declaration” (Electrohippies, 2003).

## CONCLUSION

The criteria of disobedience and justification are easily met in online environments and do not conflict with traditional theory. The issue of non-violence is a bit more complex in the sense that the non-violence can be interpreted as zero violence, however this is a flawed interpretation as zero-violence is an unobtainable goal. In the physical world we tolerate (to a varying degree) our lives being occasionally disrupted. Animal rights protesters may hamper our ability to enter into fast food restaurants, anti-war demonstrators may hinder our ability to travel through city centres as we normally do. Our daily lives are also hampered by such jubilant rugby supporters cheering the homecoming team, crowds viewing royal pageants or road-blocks and diversions set up to protect visiting politicians. Around the world on New Years Eve there is mass disobedience in the streets as the New Year is ushered in. These events are tolerated by society since they are deemed important to society. These limitations are not interpreted as violence to property and therefore nor should the activities which delay our online activities be seen as such. The main issue is one of the moral right (or obligation) to react within a globalised civil society.

Within traditional theory the protester would ideally be reacting to either to a moral wrong or withdrawing support for a government carrying out morally wrongful acts. This limitation should not, however, prevent the actions of those who protest in the name of others. The a-national nature of information technology has the effect that it can be used to conduct global protests to aid those who are unable to create a moral majority within their own nation state.

The politically motivated online disobedient is actively partaking in a political discourse, the goals of this discourse is to create a more equitable society. The disobedient is exercising fundamental rights of expression. Traditionally such rights are not limited without serious cause. The present legislative trend which criminalises online civil disobedience is too far reaching and seriously hampers the enjoyment of individuals civil rights. The blanket limitation of civil rights within a society should only be tolerated if the limitation also has the effect of removing a serious threat to the society which faces those limitations. The threat of online crime has been greatly overstated and is founded upon a lack of understanding of the technology or even technophobia. The rush towards criminalisation should be tempered with a toleration of political discourse.

## NOTES

1. <http://web.amnesty.org/actnow/appeals-eng>
2. <http://act.greenpeace.org/>
3. <http://www.corpwatch.org/action/PHA.jsp>
4. <http://www.foei.org/cyberaction/index.html>
5. [http://gao.org/freedom\\_action/home.tcl](http://gao.org/freedom_action/home.tcl)
6. <http://www.oxfam.org.au/campaigns/nike/postcard.html>
7. <http://www.burmacampaign.org.uk/actions/un.htm>
8. [1998] AC 1063.
9. <http://www.zone-h.org/defacements/mirror/id=217086/>
10. COM(2002) 173 final. Adopted in April 2002, it provides a general framework to approximate and increase judicial and police cooperation in relation to attacks against information systems. Member states had until 31 December 2003 to implement the proposed framework.
11. Convention on Cybercrime (2001) (Treaty no. 185) requires 5 Ratifications including at least 3 member States of the Council of Europe, as of March 2004 these conditions have been met.

## REFERENCES

- AOL Press Release, *America Online Releases 'Top 10 Spam' List of 2003*, 31 December 2003. [http://media.aoltime Warner.com/media/pres\\_s\\_view.cfm?release\\_num=55253692](http://media.aoltime Warner.com/media/pres_s_view.cfm?release_num=55253692)
- Bedau, H. A. (1961) On civil disobedience. *Journal of Philosophy*, vol 58.
- Bedau, H. A. (1970) Civil disobedience and personal responsibility for injustice, *The Monist*, 54. (Reprinted in Bedau, H. A. (ed.), *Civil Disobedience in Focus*, Routledge, 1991.)
- Bedau, H. A. (ed.) (1991) Introduction. *Civil Disobedience in Focus*, Routledge.
- Electrohippie Collective (2000) *DfNZ & the action tool development group. Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act?* The electrohippies collective occasional paper no. 1, <http://www.fraw.org.uk/ehippies/papers/op1.html>
- Electrohippie Collective (2003) *Electrohippie Collective's online protest against the Iraq War*. <http://www.internetrights.org.uk/casestudies.shtml>
- Fairweather, N. B. (1999) The future of environmental direct action: a case for tolerating disobedience. In: Fairweather, Stephens, Stroh and Elworthy (eds.), *Environmental Futures*, Macmillan.
- Gandhi, M. (1942) *Non-Violence in Peace and War*. Ahmedabad, Navajivan.
- Information Commissioners (2003) *Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003 – Part 1*. <http://www.informationcommissioner.gov.uk>
- Kerr, O. (2003) Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes. *New York University Law Review*, vol. 78, p 1596.
- King, M. L. (1963) Letter from a Birmingham Jail. *Why We Can't Wait*, Harper & Row.
- Klang, M. Virtual sit-ins, civil disobedience and cyberterrorism. In: Klang, M. and Murray, A. (eds.), *Human Rights in the Digital Age*, Cavendish Publishing.
- Manion, M. and Goodrum, A. (1999) Terrorism and civil disobedience: towards an international ethic of hacktivism. *Proceedings of ETHICOMP*.
- NIPC (2001) *Cyber Protests: The Threat to the U.S. Information Infrastructure*. National Infrastructure Protection Center. <http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf>
- Plato (2002) *Five Dialogues: Euthyphro, Apology, Crito, Meno, Phaedo*, G. M. A. Grube (trans), Hackett Publishing.
- Rawls, J. (1963) Legal obligations and the duty of fair play. In: Hook, S. (ed.), *Law and Philosophy* New York, NYU Press.
- Rawls, J. (1971) *Theory of Justice*, Harvard University Press.
- Dworkin, R. (1977) *Taking Rights Seriously*, Harvard University Press.
- Oxblood Ruffin (2000) *Response to electrohippies*, Cult of the Dead Cow (2000-07-17) [http://www.cultdeadcow.com/details.php3?listing\\_id=410](http://www.cultdeadcow.com/details.php3?listing_id=410)
- Singer, P. (1973) *Democracy and Disobedience*, Oxford University Press.
- Srijith, K. N. (2002) Analysis of Defacement of Indian Web Sites, *First Monday*, vol 7, no 12. [http://firstmonday.org/issues/issue7\\_12/srijith/index.html](http://firstmonday.org/issues/issue7_12/srijith/index.html)
- Suber, P. (1999) Civil disobedience. In: Christopher B. Gray (ed.), *Philosophy of Law: An Encyclopedia*, Garland Publishing.
- Taylor, P. (1999) *Hackers: Crime in the Digital Sublime*, Routledge.
- Thoreau, H. D. (1993) *Civil Disobedience*, Dover Publications.
- Tolstoy, L. (1884) *My Religion, on life, thoughts on God and on the meaning of life*, Wiener, L. (trans), Vol. 16, *My Religion* (1884), Boston 1904.
- Volokh, E. (2003) The mechanisms of the slippery slope, *Harvard Law Review* vol 116.

## CORRESPONDING AUTHOR

Mathias Klang  
 University of Göteborg, Box 620,  
 405, 30, Göteborg, Sweden  
 Email: [klang@informatik.gu.se](mailto:klang@informatik.gu.se)

