McGill Law Journal
Revue de droit de McGill

Technological Self-Help and Equality in Cyberspace

Jennifer A. Chandler

Volume 56, Number 1, December 2010

URI: https://id.erudit.org/iderudit/045698ar
DOI: https://doi.org/10.7202/045698ar

See table of contents

Publisher(s)

McGill Law Journal / Revue de droit de McGill

ISSN

0024-9041 (print)
1920-6356 (digital)

Explore this journal

Cite this article

Chandler, J. A. (2010). Technological Self-Help and Equality in Cyberspace. *McGill Law Journal / Revue de droit de McGill*, *56*(1), 39–75. https://doi.org/10.7202/045698ar

Article abstract

New technologies challenge the law in many ways, for example, they extend one's capacity to harm others and to defend oneself from harm by others. These changes require the law to decide whether we have legal rights to be free from those harms, and whether we may react against those harms extrajudicially through some form of self-help (e.g., self-defence or defence of third parties) or whether we must resort to legal mechanisms alone. These questions have been challenging to answer in the cyberspace context, where new interests and new harms have emerged. The legal limits on permissible self-defence have historically been a function of necessity and proportionality to the threat.

However, this article argues that case law and historical commentary reveal that equality between individuals is also an important policy issue underlying the limits on self-defence. The use of technologies in self-defence brings the question of equality to the fore since technologies may sometimes neutralize an inequality in strength between an attacker and a defender. A legal approach that limits resort to technological tools in self-defence would ratify and preserve that inequality.

However, the relationship between technology and human equality is complex, and this article proposes an analytical structure for understanding it. The objective is to understand which technologies promote equality while imposing the least social costs when used in self-defence. The article proposes principles (including explicit consideration of the effects on equality) for setting limits on technological self-help, and illustrates their use by applying them to several forms of cyberspace counter-strikes against hackers, phishers, spammers, and peer-to-peer networks.

McGill Law Journal ~ Revue de droit de McGill

TECHNOLOGICAL SELF-HELP AND EQUALITY IN CYBERSPACE

*Jennifer A. Chandler**

New technologies challenge the law in many ways, for example, they extend one's capacity to harm others and to defend oneself from harm by others. These changes require the law to decide whether we have legal rights to be free from those harms, and whether we may react against those harms extrajudicially through some form of self-help (e.g., self-defence or defence of third parties) or whether we must resort to legal mechanisms alone. These questions have been challenging to answer in the cyberspace context, where new interests and new harms have emerged. The legal limits on permissible self-defence have historically been a function of necessity and proportionality to the threat.

However, this article argues that case law and historical commentary reveal that equality between individuals is also an important policy issue underlying the limits on self-defence. The use of technologies in self-defence brings the question of equality to the fore since technologies may sometimes neutralize an inequality in strength between an attacker and a defender. A legal approach that limits resort to technological tools in self-defence would ratify and preserve that inequality.

However, the relationship between technology and human equality is complex, and this article proposes an analytical structure for understanding it. The objective is to understand which technologies promote equality while imposing the least social costs when used in self-defence. The article proposes principles (including explicit consideration of the effects on equality) for setting limits on technological self-help, and illustrates their use by applying them to several forms of cyberspace counter-strikes against hackers, phishers, spammers, and peer-to-peer networks.

Les nouvelles technologies posent de nombreux défis en droit. À titre d'exemple, elles augmentent la capacité des individus d'infliger du mal à autrui, mais aussi leur capacité à se défendre du mal. Ces changements exigent du droit de décider si nous avons ou non le droit, juridiquement parlant, d'être à l'abri du mal. Le droit doit aussi décider si nous sommes libres de réagir au mal de façon extrajudiciaire, par l'entremise d'initiatives personnelles (par exemple, l'auto-défense ou la défense des tierces parties) ou si au contraire nous devons nous en tenir aux mécanismes juridiques. Ces questions posent un défi particulier dans le contexte du cyberespace, d'où émergent de nouvelles menaces et des intérêts nouveaux. Les limites juridiques de l'autodéfense permissible dépendent historiquement de la nécessité et de la proportionnalité de la réaction face à la menace.

Cet article soutient toutefois que la jurisprudence et les commentaires historiques révèlent que l'égalité entre individus constitue aussi une question de politique importante qui sous-tend les limites de l'autodéfense. L'utilisation des technologies dans l'autodéfense porte donc au premier plan la question de l'égalité puisque la technologie peut parfois neutraliser une inégalité de force entre une personne qui attaque et une autre qui se défend. Une approche juridique qui limiterait l'utilisation d'outils technologiques dans l'autodéfense entérinerait et préserverait cette inégalité.

Pourtant, la relation entre la technologie et l'égalité entre humains est complexe. Cet article propose une structure analytique pour mieux saisir cette relation. L'objectif est de comprendre quelles technologies favorisent l'égalité tout en imposant les coûts sociaux les moins élevés lorsqu'elles sont utilisées pour l'autodéfense. L'article propose des principes pour mettre en place certaines limites aux initiatives personnelles technologiques. L'article illustre aussi l'utilisation de ces principes en les appliquant à de nombreuses formes de riposte contre les pirates informatiques, les hammeçonneurs, les polluposteurs et les réseaux pair à pair. Enfin, l'article considère explicitement les effets de ces principes sur l'égalité.

* Associate Professor, Faculty of Law, University of Ottawa. I thank the anonymous peer reviewers for their useful comments and suggestions. I also gratefully acknowledge the support of ORNEC (the Ontario Research Network for Electronic Commerce) for my work on legal responses to identity theft, out of which this paper also emerged.

Citation: (2010) 56:1 McGill LJ 39 ~ Référence : (2010) 56 : 1 RD McGill 39

Introduction

Self-help refers to a set of actions that the law permits people to take in the pursuit of their legal rights. The law has long permitted various forms of self-help, including self-defence, the defence of property, and the defence of third parties, although only within cautious bounds. One area of ongoing debate regarding self-help is whether counter-strikes should be permitted in cyberspace against, for example, hackers, phishers, spammers, and peer-to-peer networks. The difficulty and inefficacy of law enforcement online—particularly in dealing with the high volume of fraud and other financial harms—has resulted in self-protection becoming the normal recourse and has also encouraged more aggressive forms of self-defence (as an alternative to invoking state protection).

Self-defence is permissible when it is necessary and when the action is reasonably proportional to the threat. The issue of the inequality in strength between parties is not an explicit consideration in assessing whether a given action in self-defence is permissible or not, although it is considered implicitly. This article argues that the issue of equality of strength—understood more broadly than physical strength alone—should be an explicit criterion for determining the proper limits on the use of technologies in self-defence.

Where an attacker and a defender are of unequal strength, a legal approach that prohibits resort to technological tools in self-defence would ratify and preserve that inequality. In these cases, technologies could neutralize the inequality in strength; for example, the nineteenth-century nickname for the Colt handgun was "the Equalizer". As is the case with the handgun, technologies may raise the risks associated with self-help and may impose other social harms while at the same time having this equalizing effect. Another problem with permitting the use of technologies in this way is that it may fuel a technological arms race, as parties seek to gain the technological advantage. Regulatory choices about such technologies and the willingness to condone their use in self-defence require a balancing of these competing considerations.

The relationship between technology and human equality is complex, and this article proposes an analytical structure for understanding it. The objective is to understand which technologies promote equality while imposing the least social costs in terms of escalating violence, accidental harm to bystanders, and wasteful arms racing. Such technologies should be permissible for use in self-defence, subject to the possible requirement that users compensate injured bystanders.

The article will proceed in the following way. First, I explain the terms "self-help", "technology", and "equality" as I define them in this analysis. Second, I propose a structure for understanding how technologies affect

human equality. Third, I propose principles—including a consideration of their effects on equality—for setting limits on technological self-defence, and illustrate their use by applying them to several forms of counter-strikes under consideration in cyberspace.

I. Defining Self-Help, Technology, and Equality

A. Self-Help

1. A Definition of Self-Help

In law, self-help is a category of actions that individuals can legally undertake without state assistance in order to protect their own legally-recognized rights. Extra-judicial self-help remedies arise in numerous areas of the law, allowing people to use force in self-defence, in defence of property—including chattels—or in defence of third parties.[1] Categories of self-help also exist to permit people to trespass on property to abate nuisances, to retrieve property, and, in certain circumstances, to destroy the property of others.[2] It is necessary here to say a few words about the separate parts of the proposed definition.

First, we are concerned in this context only with those actions undertaken in self-help that would be illegal but for a specific exemption or privilege such as, for example, self-defence or abatement of nuisance.[3] There is a whole range of legal actions that individuals may undertake in order to promote their own interests, such as using locks or building fences on their own property. This range of clearly legal activity tends not to be at issue in cases dealing with the legal limits on what may be done by way of self-help. It is nevertheless useful to keep these additional forms of legal activity in mind, as some such actions that are currently legal may be made illegal or vice versa. This is important in cases where the self-help activity involves a new form of technology. Emerging forms of unregulated technologies routinely challenge our understanding of

---

1 John Baker reports that the first known acceptance of the defence of chattels as an excuse for battery was in 1500: JH Baker, *An Introduction to English Legal History*, 4th ed (London: Butterworths, 2002) at 379, n 2, citing JH Baker, ed, *The Reports of Sir John Spelman* (London: Selden Society, 1978) vol 2 at 315, n 16.

2 See Douglas Ivor Brandon et al, "Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society" (1984) 37:4 Vand L Rev 845 (this comprehensive report covers the various self-help remedies available in various areas of US law including tort law, criminal law, commercial law, and landlord and tenant law); Richard A Epstein, "The Theory and Practice of Self-Help" (2005) 1:1 Journal of Law, Economics and Policy 1 at 15.

3 See *ibid* at 3.

what actions are legal or illegal in pursuit of self-interest, and what actions are privileged despite being illegal.

Second, an implicit part of the definition is that the interest pursued by the individual must be a legitimate interest. The meaning of "legitimate interest" is not clear, as this may be understood narrowly to mean only legally-recognized rights, or it may extend more broadly to include genuine interests that are not recognized as legal rights. One may have a genuine interest in many objectives ranging from illegal interests (e.g., to steal property), through a range of less clearly illegal interests (e.g., to access information contrary to an arguably overreaching contractual term proscribing it), to legal interests (e.g., to retrieve property that is being wrongfully withheld).

An illustration of a situation in which a person may feel justified in breaking the law to promote an interest that is not legally recognized is the following: a company may impose particular terms of use on its website to essentially make certain uses of information on the site illegal, or it may create access restrictions on its website to avoid access by persons from particular geographical locations (e.g., to avoid the application of certain laws governing permissible content).[4] A person may wish to use that information contrary to the contractual agreement or may wish to access the information from the excluded location by hacking or misleading the control system. The person who does so has no legal right to use that information. However, some people may intuitively feel that it is justifiable to breach the contract and access the information because they regard these contractual terms as illegitimate. What I am seeking by way of this example is to shed light on whether self-help permits the pursuit of interests that are not legally-recognized rights. Despite the feeling that people ought to be allowed to pursue their interests by avoiding over-reaching contractual provisions, a court that is bound to apply contract law would likely regard this pursuit as an unjustified breach of contract rather than an instance of legitimate self-help. In sum, the interests that one can pursue under the privileged cover of self-help must be one's own legally-recognized rights or those of another person.[5]

---

4 See *EBay Inc v Bidder's Edge Inc*, 100 F Supp (2d) 1058, 54 USPQ (2d) 1798 (ND Cal 2000) [*Ebay*] (the court enjoined Bidder's Edge from gathering information from eBay's website contrary to the website's terms of use. This decision has been controversial due to allegations that eBay's attempt to restrict the use of publicly accessible information was contrary to public policy).

5 The defence of third parties permits a person to use force to protect a third party. In such a case the legally-recognized interest being protected is the third party's bodily integrity.

The definition is ambiguous with respect to whether a person who is helping himself must act alone, or may act in concert with others. Richard Epstein writes that although the word self-help usually evokes the image of an individual acting alone to defend his own legal interests, there is nothing in the idea of self-help that precludes an individual or a group from acting in support of any individual or group that is subject to a wrong.[6] Although the dangers associated with self-help grow when people act in groups, an individual alone may be too weak to defend himself. The category of the "defence of third parties" contemplates that a person may act on behalf of another, and so it seems that the law contemplates at least some collective self-help action.

2. The Reasons For and Against Allowing Self-Help

Legal systems constrain the free use of force for good reasons.[7] A society in which violence may be used freely is one in which potential victims must waste resources on defences. The free use of force also has a tendency to spiral out of control, escalating into feuds as the members of defensive alliances are drawn into disputes.[8] A by-product of a legal system that prevents violent self-help is the removal of some of the advantage from those with superior strength, weapons, or social networks, and a step toward a concept of uniform rights due to all individuals in a community. The importance of ensuring that "might" does not make "right" was included as a justification to suppress self-help in Blackstone's *Commentaries on the Laws of England*.[9]

---

6 See Epstein, *supra* note 2 at 3.

7 Brandon et al write that "[t]he rationale for this concern [i.e., with self-help] remains unchanged since medieval times; self-help frequently leads to breaches of the peace, violence, and inequities" (*supra* note 2 at 853).

8 See Sir William Holdsworth, *A History of English Law*, 4th ed (London: Methuen & Co, 1966), vol 2 at 43; AKR Kiralfy, ed, *Potter's Historical Introduction to English Law and Its Institutions*, 4th ed (London: Sweet & Maxwell, 1958) at 348.

9 Sir William Blackstone, 3d ed by Thomas M Cooley (Chicago: Callaghan & Co, 1884) vol 2 at 4:

> [T]he public peace is a superior consideration to any one man's private property; and ... if individuals were once allowed to use private force as a remedy for private injuries, all social justice must cease, the strong would give law to the weak, and every man would revert to a state of nature; for these reasons it is provided, that this natural right ... shall never be exerted, where such exertion must occasion strife and bodily contention, or endanger the peace of society.

See also Milton H Aronson, "Self-Help in the Collection of Debts as a Defense to Criminal Prosecution" (1938) 24:1 Wash ULQ 117 at 117; Neal Katyal, "Community Self-Help" (2005) 1:1 Journal of Law, Economics and Policy 33 at 37.

It seems unlikely that this egalitarian impulse was the prime motivation to suppress self-help in early legal systems. Still, on the one hand—and this point is important for the following discussion on equality—by suppressing self-help the law may, to some extent, neutralize the effects of an unequal distribution of strength between people with respect to the resolution of legal disputes. But on the other hand, whether or not the suppression of self-help has this egalitarian effect depends upon the unrealistic assumption that all parties have equal access to the state's support in vindicating their rights.[10] If access to the law is so expensive that many cannot pursue their legal rights in that way, rules that restrict self-help might actually harm those who could more cheaply and effectively protect their own interests themselves.

The inclusion of technological means of engaging in self-help adds another reason to limit self-help. Technology often increases the potential destructiveness of the individual, which increases the risk that the methods employed in self-help will be excessive, or that they will harm third parties. The risks of severe damage to the target and bystanders are increased by using the gun rather than the fist, for example.

Arrayed against these reasons to suppress self-help are various reasons to permit it in some cases. Holdsworth observed that, as a historical matter, it was never possible to fully repress self-help, and he suggested it would be undesirable to do so.[11] It may be more efficient to allow someone to help himself to his rights than to require the state to intervene judicially in every dispute.[12] Another possible advantage of self-help in some cases is that the parties involved bear the costs of resolving their own disputes rather than having the public subsidize them.[13]

Apart from an efficiency argument, there is also an effectiveness argument. The judicial process may be inadequate because it is too slow or

---

[10] The assumption is unrealistic given the importance of wealth or social status, or both in accessing justice.

[11] Holdsworth, *supra* note 8 at 100, citing Sir Frederick Pollock & Frederic William Maitland, *History of English Law: Before the Time of Edward I*, vol 2 (Cambridge: Cambridge University Press, 1895) at 572.

[12] See Holdsworth, *supra* note 8 at 100:

> But, though early law can thus set conditions for the exercise of the right of self-help, no body of law can altogether repress it—nor, if it was able, would it be desirable to do so. If the individual can be allowed to help himself quietly to his rights without disturbing the general public, if as a rule the individual does not try to help himself unless he has right on his side, it will save time and trouble if the individual is allowed to act.

[13] See Celia R Taylor, "Self-Help in Contract Law: An Exploration and Proposal" (1998) 33:4 Wake Forest L Rev 839 at 848.

offers unsuitable remedies.[14] Self-defence must be permitted because the victim who is threatened with a violent attack cannot wait for the state to intervene.[15] Situations where the state could be effective but has inadequate resources and so does not offer adequate remedies are more difficult to assess. Should people be allowed to resort to self-help in these cases? Situations of this type are common in cyberspace.[16] One may argue that a system that suppresses self-help, but does not provide adequate state protection of legal rights, invites violations of those rights since there is no credible deterrent when victims cannot engage in self-help.[17]

Given these competing reasons for and against self-help, the law has taken a fairly loosely defined position toward self-help—centred on the concepts of necessity, reasonableness, and proportionality.[18] The following points can be extracted from a review of the various rules on self-help:[19]

- Only certain legal interests can be defended using force. These include the protection of property and the person against physical interference, and the protection of the use and enjoyment of prop-

---

[14] Brandon et al note that various self-help remedies have persisted over the years, usually where the judicial remedies are inadequate and "the threat of a self-help remedy to ... law and order is minimal" (*supra* note 2 at 853).

[15] See Blackstone, *supra* note 9 at 2-3:

> But as there are certain injuries of such a nature, that some of them furnish and others require a more speedy remedy than can be had in the ordinary forms of justice, there is allowed in those cases an extrajudicial, or eccentrical kind of remedy
>
> ...
>
> It considers that the future process of law is by no means an adequate remedy for injuries accompanied with force; since it is impossible to say to what wanton lengths of rapine or cruelty outrages of this sort might be carried, unless it were permitted a man immediately to oppose one violence with another.

[16] For example, should banks be allowed to attack phishing websites to take them down? Phishing websites pose a continual problem because they simply reappear elsewhere online when they are successfully taken down. If the state has bigger problems to address, should private parties be allowed to use self-help against such problems in cyberspace?

[17] Epstein, *supra* note 2 at 29: "To ask an innocent party ... to refrain from the use of force when threatened with serious bodily harm or the substantial loss of property is to demand too much, and to increase the chances of such aggression."

[18] *Ibid* at 28 (noting that self-help is more likely to be tolerated where there is a back-up procedure available to contest the legality of self-help action).

[19] Brandon et al, *supra* note 2; Allen M Linden & Bruce Feldthusen, *Canadian Tort Law*, 8th ed (Markham, Ont: LexisNexis Canada, 2006); Dan B Dobbs, *The Law of Torts*, vol 1 (St. Paul, Minn: West Group, 2001).

erty against unreasonable interference.[20] The self-help categories of self-defence, the defence of third parties and the defence of property are available to defend against physical interference with the person and with property. Abatement of nuisance is available to deal with unreasonable interferences with the use and enjoyment of property.

- There must be no acceptable alternative response to the threat other than the use of force.[21]
- The degree of force used must be reasonable and may not be greater than is reasonably necessary to meet the threat.[22]
- The degree of force used must be proportional to the threat. For example, it is unacceptable to use deadly force to protect property, and compensation may be due for personal injuries caused while protecting property interests.[23]
- There are various rules applicable to these self-help remedies that are designed to avoid mistakes and unnecessary violence: In some cases, a warning or request to desist must be given before resort to the use of force. In other cases, it is necessary to pay compensation where a mistake is made.[24] Still other rules are designed to try to limit harm to bystanders, including the rule that compensation must be paid where harm is inflicted negligently by a party acting in self-defence.

---

[20] The cases on self-help usually deal with "real-world" physical interference. However, in other cases dealing with cyberspace, the courts have accepted that trespass to chattels may be committed electronically over the internet. See e.g. *Ebay*, *supra* note 4. This suggests that at least some of the legal principles designed for the physical world will be transposed into cyberspace. While some courts have accepted that physical property such as servers might be subject to electronic forms of trespass, it is less clear whether intangible property such as intellectual property or information can be trespassed upon, let alone whether it is a type of property that may be defended using force.

[21] See *Restatement of the Law (Second) Torts* §63 (1965) [*Restatement*] (see comments, k, l, m); Brandon et al, *supra* note 2.

[22] See *Restatement*, *supra* note 26 §70.

[23] See Brandon et al, *supra* note 2 at 862, 870; *Restatement*, *supra* note 21 §75; Dobbs, *supra* note 19 at 170 (even if one is absolved of liability toward one's attacker for actions in self-defence, one may still be liable in negligence if a bystander is harmed); Linden & Feldthusen, *supra* note 19 at 89.

[24] See Brandon et al, *supra* note 2 at 861, 864.

B. A Definition of Technology and "Technological Self-Help"

The definition of "technology" is not settled. Some define the scope of the term broadly to include all tangible and intangible tools and techniques. A narrow definition would regard technology as limited to the physical artifacts created and used by humans as tools to achieve their objectives.[25] Jacques Ellul has chosen a broader definition that he labels "technique", in which he includes any method adopted by humans to achieve a goal more efficiently in any field of human activity.[26] This latter definition would include not only physical artifacts, but also methods and organizational structures, among other things. Don Ihde adopts an intermediate ground, requiring that technology include a material component, but extends his definition to the methods or techniques that use the material artifact.[27]

For the purposes of my inquiry into technological self-help, I will adopt Ellul's broader definition for two reasons. First, existing case law on self-help makes it clear that the adoption of non-material techniques such as martial arts is relevant to the court's reasoning.[28] As a result, the use of techniques, and not only material objects like guns, has already been proven relevant to the analysis in this context. Second, there is some uncertainty in cyberspace—and in the law in general—on how to understand non-material forms of property, such as data or intellectual property. There is also some debate over how to characterize novel forms of interference and nuisance over the Internet.[29] The courts, at least in the United States, have chosen to regard electronic communications over the Internet as capable of falling within the scope of trespass to chattels; a category that was formerly understood to involve a physical—presumably non-electronic—form of interference.[30] Excluding non-material techniques

---

[25] See Stephen J Kline, "What Is Technology?" (1985) 5:3 Bulletin of Science, Technology & Society 215; Frederick Ferré, *Philosophy of Technology* (Athens, GA: University of Georgia Press, 1995) at 14-29.

[26] Jacques Ellul, *The Technological Society*, translated by John Wilkinson (New York: Vintage Books, 1964) at xxv.

[27] Don Ihde, *Philosophy of Technology: An Introduction* (New York: Paragon House, 1993) at 47.

[28] For example, the Saskatchewan Court of Queen's Bench pronounced on the use of karate in defence of another. See *Cachay v Nemeth* (1972), 28 DLR (3d), 603 (Sask QB) [*Cachay*] (the court held that "[t]he blow, struck as it was by one who had been trained in Karate ... was out of proportion to the apparent urgency or requirement of the situation" at para 7).

[29] See Dan L Burk, "The Trouble With Trespass" (2000) 4:1 J Small & Emerging Bus L 27. For a useful summary of the debate as reflected in the case law and scholarly commentary, see Guy Lastowka, "Decoding Cyberproperty" (2007) 40:1 Ind LR 23.

[30] See *Ebay*, *supra* note 4.

from technological self-defence thus fails to reflect current legal practice as well as more novel and uncertain areas of self-defence and defence of property, such as cyberspace.

Apart from these reasons, it is my view that many important tools need not involve physical artifacts (e.g., languages, mental heuristics, recipes, etc.), and that sometimes where there is a physical artifact, the artifact is really secondary to the central tool. For example, the physical manifestation of a software program is essentially irrelevant. It does not matter, to an understanding of the technological aspect of the software, whether it resides on a USB key or a CD. It is true that while software is operating, it does so through various physical machines, and those machines become an important part of understanding the effects of the combined artifact and technique.

Under the broader definition the legal system itself, with its language, rules, institutions, and artifacts, is a type of social technology: It is a tool that different actors use for different purposes. It is a system that individuals—by invoking the state apparatus to defend and enforce rights—may use to try to pursue their legal rights. Technological self-help can thus be understood as the use of tools other than the legal system to pursue legal rights. Technological self-help nonetheless remains part of the legal system since self-help is simply a set of legal rules defining a category of actions that a person can legally undertake without state assistance in order to protect his own legally-recognized rights.

C. A Definition of Equality

Equality is a central component of the main normative theories of social arrangement, even if the concept of equality varies from theory to theory.[31] For instance, one theory's demand for equality in one dimension may conflict with another's demand for equality in another. Nevertheless, equality—in some dimension—remains a central requirement since a justifiable theory of social arrangements must be acceptable from the perspectives of all affected.[32]

Various forking points present themselves when one tries to choose a concept of equality. First, it is necessary to choose the dimensions in which equality will matter most. By definition, when people are equal they continue to differ in some dimensions, otherwise equality would col-

---

[31] See Amartya Sen, *Inequality Reexamined* (Cambridge, Mass: Harvard University Press, 1992) 12.

[32] See *ibid* at 17-18.

lapse into identity.[33] The challenge lies in determining which dimensions ought to be the same in order that people can be said to be equal, and which dimensions may remain different. People may differ in various dimensions,[34] although they are likely to care only about valuable variables such as resources, well-being, or rights—like liberty.[35] The objective in this paper is to consider the effects of rules regarding technological self-help on equality. In order to make the inquiry more manageable, I will consider the way in which technologies equalize resources, since one's resource endowment will have a direct effect on the ability to pursue one's legal interests. I take resources to include both external and internal resources, since technologies are available to affect both. External resources include factors such as wealth, the characteristics of the surrounding natural environment, and the social and cultural resources provided by the surrounding community. Internal resources are internal or personal characteristics, such as age, sex, personality, and physical or mental abilities.

Another choice to be made is whether we are concerned with equality of outcome or equality of opportunity. I think that the proper way to understand the concern at the heart of the question of whether technological self-help of one kind or another should be permitted is that there should be equal opportunity to pursue one's legal rights. On the one hand, a theory of equality that suggests that equality of opportunity is the central objective is open to criticism. It could, for example, justify highly unequal outcomes with respect to the actual protection of legal rights, as factors such as luck and effort lead to different results for different people. On the other hand, the pursuit of equality of outcome leaves no room for personal

---

[33] See Stefan Gosepath, "Equality" *Stanford Encyclopedia of Philosophy* (1 December 2009), Edward N Zalta, ed, online: <http://plato.stanford.edu/entries/equality/> at para 1.

[34] See Sen, *supra* note 31 at 19-21. Sen writes that "[l]iberties, rights, utilities, incomes, resources, primary goods, need-fulfilments, etc., provide different ways of seeing the respective lives of different people, and each of the perspectives leads to a corresponding view of equality" (*ibid* at 25).

[35] See Joseph Raz, "On the Value of Distributional Equality", in Stephen de Wijze, Matthew H Kramer & Ian Carter, eds, *Hillel Steiner and the Anatomy of Justice* (New York: Routeledge, 2009) 22 at 25, n 7:

> Egalitarians are by necessity pluralists about value. According to them there is value only in the distribution of something which is in itself of (some) intrinsic value, that is something whose value is independent of equality ... The beginning of the proof [of this] is to note that there is no value in the equal distribution of something which is itself neither good nor bad, like the number of hairs to be found on one's shirts at any given time. To be plausible at all the value of equality must relate to the distribution of items like food, opportunities for valuable activities, freedom, and other things of value independently of their distribution.

responsibility, such that society would have to continually channel more resources to those who squander their resources and opportunities.[36] By including the concept of internal resources, above (which include talent and personality, as well as all the contextual factors like social oppression or social support that may affect a person's ability to actively pursue opportunities), I hope to address the critique that equality of opportunity ignores the problem of unequal starting points with regard to factors related to personal responsibility.[37]

II. The Relationship Between Technology and Equality

This article is focused on understanding when a technology should be legally permissible for use in self-help, and on proposing that a technology's effects on equality be considered in making that decision. Therefore, it is necessary to explain further how we might understand the effects of technology on equality.

The most familiar story about the relationship between technology and equality is neatly summarized by the term "the Digital Divide". The term, referring to the unequal global pattern of internet access, expresses the idea that technologies are usually beneficial to people, and so inequality may develop between those who have access to those benefits and those who do not. This story is accurate, since the issue of access to beneficial technologies is an omnipresent feature of the relationship between equality and technology. However, the relationship between equality and technology is more complex than this, as discussed later in this section.

A complete theory of equality needs to explain whether equality should be promoted only among human beings or among a larger set—including other living beings. Science and technology complicate this picture by, for example, revealing the genomic similarity between humans and other animals, as well as making it possible to combine human and animal genes.[38] A complete theory of equality must also deal with the problem of time: Are humans of all ages to be treated equally? Is the equality of present and future generations to be a concern? Technologies are highly relevant to equality among humans over time. Not only are we increasingly capable of manipulating the genetics of future generations of

---

[36] See Richard J Arneson, "Equality" in Robert L Simon, ed, *The Blackwell Guide to Social and Political Philosophy* (Malden, Mass: Blackwell, 2002) 85 at 94.

[37] See *ibid* at 98.

[38] See Robert H Waterston et al, "Initial Sequencing and Comparative Analysis of the Mouse Genome" (2002) 420:6915 Nature 520. The fact that it is technologically possible to create human-animal chimeras led to a legal response in Canada. See *Assisted Human Reproduction Act*, SC 2004, c 2, s 5(1)(i).

humans, but our technologies are also deeply implicated in the environmental modifications that present generations will leave for future generations. These themes are fascinating, and they may be relevant to self-help, particularly if inheritable genetic self-modification can be understood as a form of self-help. However, I will set aside the problems of time and the equality of present and future generations to consider the effects of technology on the equality between current human beings.

There is a difficulty in making pronouncements about the general effects of technology on equality—although one can fairly confidently say that it is generally true that inequality of access to technology (mostly beneficial in some way) undermines equality. However, it is still important to look at technologies individually, since they differ in their effects on human equality. Some technologies increase equality, some diminish equality, and some do both. Another useful dimension to consider in the study of the limits on permissible self-help is whether or not—apart from its relationship with equality—the technology provides a net benefit at the social level. In other words, there may be some technologies that are, in the aggregate, beneficial to society even if they decrease equality, or other technologies that are, in the aggregate, harmful even if they increase equality. In these cases, when deciding legal policy, it is necessary to face the difficult decision of which values should be given pre-eminence. Will we "purchase" more equality at the expense of some other value?

The following chart explains the relationship between technology and equality through specific examples. This chart is an over-simplification of the real relationship between technology and equality, although I do think it identifies some of the complexity and goes further than the story of the "Digital Divide" in explaining the relationship.

	PROMOTE EQUALITY	DECREASE EQUALITY
NET POSITIVE EFFECT ON SOCIETY	Example: The discovery of insulin and methods to produce it.	Example: The invention of the Internet and the "Digital Divide".
	Insulin is of use primarily to diabetics and permits them to achieve improved health. Its use partly closes a health gap between diabetics and non-diabetics.	The Internet permits those who enjoy access to benefit from improved access to information and communication, while those without access remain in the same position as before.
NET NEGATIVE EFFECT ON SOCIETY	Example: The handgun.[39]	Example: The sport utility vehicle (SUV).
	The nineteenth-century name for the Colt handgun was "the Equalizer", due to its ability to level the field in a fight between opponents of unequal strength. At the same time, the increased use of the handgun in disputes between opponents has raised the risks of injury for bystanders.	By switching to an SUV from a car, the occupants of an SUV lower their risk of fatality in a crash with a car, while raising the risk for the occupants of the car and other users of the road. In fact the increase in risks to others is greater than the decrease in risk for the SUV driver—producing a negative net effect overall.[40]

[39] The claim that guns increase the rate of death and injury in a population is controversial; see e.g. Janet Weiner et al, "Reducing Firearm Violence: A Research Agenda" (2007) 13:2 Injury Prevention 80. However, if the claim is true, then the handgun would provide an example of a type of technology that can—to some degree—neutralize a disparity in physical strength between opponents, while at the same time raising risks to others (e.g., through accidents).

[40] I draw this example from Frank Pasquale's insightful discussion of the interesting work of Michelle White:

> [F]or each fatal crash involving occupants of their own vehicles that drivers avoid by choosing light trucks, more than four additional fatal crashes occur involving car occupants, pedestrians, bicyclists, and motorcyclists. In other words, safety gains for those driving light trucks come at an extremely high cost to others (Michelle J White, "The 'Arms Race' on American Roads: The Effect of Sport Utility Vehicles and Pickup Trucks on Traffic Safety" (2004) 47:2 J L & Econ 333 cited in Frank Pasquale, "Technology, Competition, and Values" (2007) 8:2 Minn J L Sci & Tech 607 at 608).

There are four important caveats to this conceptual structure that I can see, doubtless there are more. First, the equality that matters to people is a multi-faceted entity (e.g., happiness, welfare, power, and wealth), and the achievement of equality in the one or two dimensions that an individual technology may enable may be relatively unimportant. Clearly, one cannot declare the weak and strong equal once the weak have handguns. This is not just because the handgun is only useful in some—but not all—circumstances where strength is called for, but because equality in strength is not the only or even the most important dimension in which people may wish to be equal.

Second, regardless of whether or not a technology is able to increase equality in a given dimension such as strength, the question of access to the technology will still remain. In other words, the mere existence of a technology that could equalize a disadvantage is not useful in itself; it accomplishes equalization only if it is reasonably affordable and accessible to those who are disadvantaged. Given the strong correlation between vulnerability, ill health, lower levels of education, and wealth, the equalizing effects of technologies may in many instances be theoretical.

Third, it is also possible that one given technology may increase equality in one dimension while simultaneously decreasing it in another dimension, as between two people. For example, to build on the SUV example above, larger vehicles are useful for people with physical disabilities, both in terms of embarking and disembarking as well as in terms of transporting wheelchairs or other equipment. However, motorists in larger vehicles impose higher accident risks on motorists in smaller vehicles. In this case the larger vehicle simultaneously increases equality in mobility while decreasing equality in terms of the risk of fatal accidents.[41]

Fourth, before celebrating the equalizing effects of a technology, it is necessary first to ask what is being equalized. If a disadvantaged group is offered a technological means to "fix" a purely socially-constructed disadvantage, it is unclear that such an opportunity would promote equality. Instead, it tends to reinforce the arbitrary view that a given characteristic is undesirable and ought to be "fixed". Consider, for example, hymenoplasty, the so-called "virginity restoration surgery".[42] On the one hand, it promotes female equality by freeing women from the effects of a sexual

---

[41] Many thanks to the attendees of the Notre Dame Law School Speakers' Series, at which I spoke in the winter of 2009, for suggesting the category of technologies that simultaneously increase and decrease equality in different dimensions.

[42] See William Saletan, "Sex, Lies, and Virginity Restoration", *Slate* (11 June 2008), online: <http://www.slate.com/id/2193353/>.

double standard that requires female but not male virginity.[43] On the other hand, it reinforces the double standard for other women who must also then comply with the standard or obtain the surgery.[44]

Numerous other technologies play the paradoxical role of strengthening a socially-constructed discriminatory standard at the same time as they enable those disadvantaged by that standard to elude its effects. Another example comes from the government-approved use of human growth hormone, not for those with a hormone deficiency, but for healthy children whose projected adult height would place them in the lowest percentile of height among adults.[45] In seeking to avoid the social stigma attached to shortness and to satisfy the social expectation of height, consumers of this hormone maintain the socially-constructed disadvantage and also increase pressure on the remaining short people to conform.

To conclude with the fourth point, if all a technology does is to permit a disadvantaged group to remedy a purely socially-constructed disadvantage then very careful thought should be given to whether this is a good or bad thing. It is difficult to shift these social constructions, and individuals may prefer to use the technology to "fix the defect" rather than hold out until society changes. Still, if a disadvantage is not purely socially constructed, and can legitimately be viewed as a disadvantage impeding the fullest possible human fulfillment, then I think we may look at the technology as potentially positive in promoting equality.

Turning to the question of how the relationship between technology and equality influences technological self-help, it is clear that if a person starts from a position of superior strength and still employs a technology that further increases the disparity, this will not be permissible. For example, a stronger person should not need to use a knife or a gun to defend against an attack by a weaker person. The court is likely to view the use of a weapon in such cases as an unreasonable or unnecessary use of force. Put another way, the adoption of a technology that increases inequality is unlikely to and ought not to be viewed favourably. But, the use of a technology that helps to level the playing field against a stronger attacker is more likely to be acceptable. Whether a technology that promotes equality in such circumstances will be acceptable for use in self-help will depend upon whether it imposes a negative net social effect, such as through the escalation of violence or harm to bystanders.

---

[43] See *ibid.*

[44] See Clare Chambers, "Autonomy and Equality in Cultural Perspective: Response to Sawitri Saharso" (2004) 5:3 Feminist Theory 329.

[45] See Michael J Sandel, *The Case Against Perfection: Ethics in the Age of Genetic Engineering* (Cambridge, Mass: Belknap Press, 2007) at 16-19.

III. Principles for Technological Self-Help

A. Proposed Principles for Technological Self-Help

The law tends to permit self-help where the law is either ineffective or inefficient in protecting a set of legal interests that are viewed as sufficiently important for society to run the risks of allowing self-help. Over time, the law has devised a series of principles to limit the scope of permissible self-help. The general principles were discussed above in the section on self-help, and pertain to the types of legal interests that can be defended using force, the requirement that there be no acceptable alternative response, and the requirement that the degree of force used be both reasonably necessary and proportional to the threat. In addition, rules regarding warnings, requests to desist, and compensation also serve to avoid mistakes and to limit unnecessary violence. In reaching and applying these principles, courts have not made technology or equality the explicit focus of this analysis, although both are implicit considerations in some cases.

With respect to technology, many actions taken in self-help employ some type of technology. As defined in this article, a technology is a tool or method (ranging from the very simple, or nearly invisible, to the novel and startling) that is deliberately used to achieve a goal. Apart from cases involving fist fights, other attempts at self-help will often employ a technology of some sort. Therefore it has been necessary—even if only implicitly—to consider the appropriate limits on technological self-help. For example, courts have had to rule on whether to permit self-defence using various types of physical artifacts (e.g., a knife)[46] or methods (e.g., karate).[47]

As for human equality, the rules on self-help do not explicitly mention this as a factor in the analysis. However, inequality is relevant at several steps of the analysis. In particular, inequality in strength and power is relevant to determining whether it is reasonable to perceive a threat and whether the degree of force used in self-defence is reasonable. Courts already implicitly consider disparity in strength between the parties when they assess whether the use of a given weapon was disproportionately violent or not. For example, a stronger person is not justified in exerting his full strength against a weaker one.[48] However, a weaker person is justi-

---

[46] See *R v BEN* (2000), 190 Sask R 109 (Sask Prov Ct) (the court accepted the use of a knife in self-defence).

[47] See *Cachay*, *supra* note 28.

[48] See *Johnson v Erickson*, [1941] 2 WWR 524, [1941] 3 DLR 651, cited in Linden & Feldthusen, *supra* note 19 at 89.

fied in using a weapon against a stronger person where it is reasonably believed to be necessary.[49] The judicial attention to the psychological effects of battered woman syndrome, for example, in assessing the reasonableness of a woman's actions also illustrates the relevance of power and strength imbalances in determining the boundaries of self-help.[50] These cases do not tend to declare the use of a particular weapon to be generally justified or not. Instead, they consider the inequality between the parties when determining whether the use of a weapon is reasonable in those circumstances, given that inequality in strength. This seems to be a reasonable approach because a judicial decision to outlaw resort to a given weapon in all cases would essentially preserve and ratify the existing unequal distribution of strength between the two people.

In this paper, I am suggesting that one factor that ought to be more explicitly considered when determining whether resort to a particular technology for self-help is acceptable is the level of inequality between the parties and the effect of the technology on that equality. I believe it is worthwhile to consider this more systematically and explicitly than has been the case where courts have dealt with individual instances of violent self-defence by a weaker party against a stronger attacker because there are other forms of inequality that may be relevant in different contexts. As discussed further below, inequalities in physical strength are not the operative inequalities in cyberspace, and it is worthwhile asking what problematic inequalities may exist in cyberspace that would benefit from technological amelioration.

At the same time, when choosing principles for technological self-help, it is important to pay attention to the ways in which technological evolution may upset the balance struck by the existing rules on self-help. Technological development may raise the risks associated with self-help. As more elaborate and destructive weapons are adopted, the risk of disproportional damage and harm to bystanders can increase, although this is not invariably true. To the extent that technological development permits more proportionate responses and more accurate targeting, so as to avoid innocent bystanders, it may lower the risks associated with self-help. As a result, whether or not a given technological tool should be permitted for use in self-help should be assessed according to the tool's characteristics.

---

[49] See e.g. *R v Chase*, [1997] NSJ No 141 (NSSC) (defendant was justified in striking his bigger and more powerful uncle in the head with a baseball bat. The court noted that the defendant was younger and slight in build, and that the uncle was a bouncer who studied martial arts and lifted weights).

[50] See e.g. *R v Malott*, [1998] 1 SCR 123 at paras 18-21, 155 DLR (4th) 513.

To the extent that technological self-help is permitted there is an incentive to engage in technological arms racing. It is unclear whether these arms races are wasteful or productive, given that they may spur useful innovation.[51] However, it may sometimes be thought good policy to declare a winner of the arms race by law in order to stop a wasteful race. Douglas Lichtman points to the *Digital Millennium Copyright Act*[52] as an attempt to stop the arms race between copyright owners seeking to use technological protections against copying and those seeking to break the protections.[53] The development of peer-to-peer (P2P) file-sharing networks was an arms race in which

> copyright holders us[ed] mislabeled decoy files to pollute the new networks, while network designers worked to build reputation information into their architecture such that a user tricked by a decoy file could warn other users not to download that false file or even interact with the trickster who introduced it.[54]

It is possible that some of this technological competition has produced useful innovation with respect to reputation and trust systems. Whether or not a given arms race is wasteful or productive will likely vary according to the specific technology and context.

The development of technologies that permit individuals to avoid or prevent harm through self-help provides the state with a reason to withdraw from addressing the harms itself. Writing about the constitutionality of government regulation of online speech, Tom Bell makes the argument that "[t]he mere possibility that user-based Internet screening software would 'soon be widely available' was relevant to our rejection of an overbroad restriction of indecent cyberspeech."[55] This was because the existence of technological solutions showed either that the state did not have a compelling need to restrict speech or that there were less restrictive means for the state to achieve its compelling objectives.[56] Bell writes that the existence of cost-effective technological solutions to a problem should militate against state intervention.[57] While this seems like good advice,

---

51 See Douglas Lichtman, "How the Law Responds to Self-Help" (2005) 1:1 Journal of Law, Economics and Policy 215 at 236.

52 Pub L No 105-304, 112 Stat 2860 (1998).

53 *Lichtman*, *supra* note 51 at 232.

54 *Ibid* at 233 [footnotes omitted].

55 *United States v Playboy Entertainment Group*, 529 US 803 at 814, 146 L Ed 2(d) 865 (2000), cited in Tom W Bell, "Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence" (2003) 87:3 Minn L Rev 743 at 746, n 15. See also Lichtman, *supra* note 51 at 216-17.

56 Bell, *supra* note 55 at 746.

57 *Ibid* at 749.

given resource constraints and all of the other things the state could be doing, it is important to scrutinize the effects of such a tendency. If the technological solution is not easily available or usable by all, there will remain a group that cannot protect itself. In addition, Bell's example involves the application of a technological solution that is lawful and low risk, whereas other technological solutions enabling individuals to prevent or avoid harms might be less benign. In those cases, state law enforcement may be a preferable way to deal with the harm.

In sum, the principles for technological self-help should build on the familiar rules of self-help, but they should also take into consideration the ways in which the concerns at the heart of those rules are affected by technologies. In addition, the concern with equality—already latent within the rules of self-help—should be understood in a broader way that permits it to help with setting appropriate rules for self-help activities in novel areas such as cyberspace. The proposed modifications and additions to the familiar rules are the following:

- Only certain legal interests can be defended using force. The law clearly accepts the protection of property and of the person from physical interference, and the abatement of nuisances.

  As technological change alters society and the kinds of harm that affect people, we may need to understand these concepts differently. For example, the increasing collection of personal information renders individuals vulnerable to its misuse. The law should contemplate the possibility that defence of the person might extend to self-defence against invasions of privacy, and the collection and misuse of personal information. As another example, the importance of information suggests that data perhaps ought to be understood as property, so that interference with stored data (e.g., corruption of data through hacking or malware) could be met with self-help in the form of abatement of nuisance or defence of property. Similarly, interferences through electronic means may now be sufficiently harmful to justify a self-help response even if prior case law mostly dealt with physical trespasses.[58]

- To the extent that the technology's use is to be permitted, rules regarding bystander compensation should be strengthened. Though the increased destructiveness of a new technology militates against permitting its use in self-help due to the increased

[58] Although trespass to chattels traditionally dealt with physical interferences, some more recent US cases have treated electronic interferences as a form of trespass to chattels: see e.g. *Ebay*, *supra* note 4.

risk of harm to bystanders, the increased specificity of a technology (i.e., better targeting) militates in favour of permitting its use in self-help since it reduces the risk of harm to bystanders.

- Concerns regarding fuelling an arms race by permitting the use of a technology in self-help must be balanced against the possibly beneficial effects of innovation that results from the arms race.
- Technologies that decrease inequality should be permissible when used in self-help by disadvantaged persons, even if their use by others would be unacceptable because they would be considered disproportionate. An example here is the judicial acceptance of resort to a handgun by a physically weaker person in defence against a stronger person.

However, as technological evolution continues to shift the nature of human interaction and competition, and the nature of the harms that people may cause to each other, it is necessary to consider inequality in other dimensions than physical strength. As discussed below, the forms of interaction and types of harms that may be caused over the Internet are different from the standard example of a physical fight: inequality may consist not in physical strength but in bandwidth. Should technological responses that amplify the offensive ability of a defender be permissible?

B. Some Forms of Self-Help in Cyberspace

There are many cyberspace examples of disagreement over the proper limits of self-help. Cyberspace provides a particularly rich context within which to consider self-help because law enforcement has tended to be ineffective in combating various kinds of Internet-borne harms. It is challenging for law enforcement authorities to respond to these harms as they often demand a high degree of technical expertise of the police, and may also involve multiple jurisdictions. In addition, with the exception of child pornography, these harms tend to involve financial loss rather than physical violence, and so may be viewed as less deserving of the investment of law enforcement resources.

The *CSI Computer Crime & Security Survey* (CSI report), now in its thirteenth year, reports that in 2008 only twenty-seven per cent of respondents reported cyber attacks to law enforcement.[59] About half of the respondents stated that they "[d]id not believe that law enforcement could

---

[59] Robert Richardson, *CSI Computer Crime & Security Survey: The Latest Results from the Longest-Running Project of its Kind* (CSI, 2008) at 22, online: Computer Security Institute <http://www.gocsi.com/survey>.

help in the matter."[60] The CSI report states that "this doesn't say good things about general perceptions of the capability of law enforcement agencies to deal with cybercrime."[61]

As a result, individuals and organizations are, to a considerable extent, left to look after their own interests rather than being able to depend upon state intervention. Indeed, a large security service sector has developed to offer privatized protection for a fee. These services largely center on defensive strategies, but the question of whether it is permissible to use offensive measures against these harms resurfaces repeatedly. In some cases, the aggressive measures are undertaken by the victim himself, by a third party who has been hired to protect the victim, or by so-called "cyber-vigilantes" who act on their own initiative.

The proper limits of self-help in cyberspace are currently unsettled. There is no consensus on whether it is acceptable to hack back against someone who is attacking your computer, or whether it is acceptable to disable a computer or network that is infringing your copyright, trafficking in stolen information, circulating malicious code, or trying to "phish" your customers.

In the following sections, I will briefly describe some of these debates, before going on to consider how the proposed self-help principles might apply to some of these cases.

1. Denial of Service Attacks

A denial of service (DoS) attack refers to the act of sending an overwhelming amount of Internet traffic to a target so that the target is disabled and prevented from undertaking normal communications. Sometimes the objective is not to completely disable a site, but instead to slow normal communications—a practice known as "bandwidth hogging". These attacks are usually launched simultaneously from many computers in a distributed denial of service attack (DDoS). The deliberate launch of a DoS attack is a crime in numerous countries including Canada, the United Kingdom, and the United States.[62] Nonetheless, DoS or its more

---

60 *Ibid* at 23.

61 *Ibid*.

62 See *Criminal Code*, RSC 1985, c C-46, s 430(1.1); Computer Misuse Act 1990 (UK), c 18, s 3; *Crimes and Criminal Procedure*, 18 USC § 1030(a)(5)(A) (2008). See also Scott Effringham, ed, *Prosecuting Computer Crimes* (Computer Crime and Intellectual Property Division Section, Criminal Division Office of Legal Education Executive Office for United States Legal Attorneys, 2007), online: <http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf>.

moderate version "bandwidth hogging" have, on occasion, been used as a form of self-help.

In early 2000, Conxion Inc., which hosted the server of the World Trade Organization (WTO), responded to an attack launched by the Electrohippies by redirecting the attack back to the E-hippies' server.[63]

Several attempts to deal with spam using DoS or bandwidth hogging have also been made. In 2004, Lycos launched an anti-spam campaign that offered its users a screensaver program that would use idle computing power to repeatedly contact spammers' websites.[64] The screensaver apparently had some success against spammers, taking several spam websites offline, although Lycos maintained that it was not engaged in DoS, but was just slowing bandwidth to increase the cost of spamming.[65] Nonetheless, spammers quickly responded, attacking the site offering the screensaver and circulating malware masquerading as the screensaver.[66] Various "vampire" programs, such as SpamVampire and LadVampire, were also programs that would repeatedly re-load a spammer's website or the website of a company being advertised through spam.[67]

The bandwidth hogging technique has been used against sites engaged in online fraud.[68] Certain forms of online fraud, such as phishing or advance fee fraud (also known as 419 fraud), make use of false financial

---

63 See Vikas Jayaswal, William Yurcik & David Doss, "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?" (Paper delivered at the International Symposium on Technology and Society, Raleigh, NC, 6 June 2002), IEEE at 381, online: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01013841>; Pia Landergren, "Hacker Vigilantes Strike Back", *CNN* (20 June 2001), online: <http://archives.cnn.com/2001/TECH/internet/06/20/hacker.vigilantes.idg/index.html>.

64 See Munir Kotadia, "Spammers Hack Lycos' Anti-spam Web Site", *ZDNet* [Australia] (1 December 2004), online: <http://www.zdnet.com.au/news/security/soa/Spammers-hack-Lycos-anti-spam-Web-site/0,130061744,139168558,00.htm>.

65 See Dan Ilett, "Antispam Screensaver Downs Two Sites in China", *ZDNet* [United Kingdom] (2 December 2004), online: <http://www.zdnet.com/news/antispam-screensaver-downs-two-sites-in-china-140070?tag=content>.

66 See *ibid*; John Leyden, "Fake Lycos Screensaver Harbours Trojan", *The Register* (7 December 2004), online: <http://www.theregister.co.uk/2004/12/07/fake_lycos_screensaver_trojan/>.

67 See Brian McWilliams, "Chongq and the Spam Vampires", *O'Reilly* (3 December 2004), online: <http://www.oreillynet.com/pub/a/network/2004/12/03/chongq.html>. See also "Pick Your Poison", online: theScamBaiter: Fighting Scammers Worldwide for Fun and Justice <http://www.thescambaiter.com/antispam/>. Scambaiter invites people to target Alex Polyakov, an alleged spammer: "We need 5000 people all running SpamVampire for a few months to beat him, so tell everyone you know (*ibid* at "SpamVampire")."

68 See "Muguito User's Manual", online: Artists Against 419 <http://wiki.aa419.org/index.php/Muguito_users'_manual>.

websites.[69] In the case of phishing, once a company or institution learns that its customers are being targeted, it is important to stop the attack as quickly as possible in order to minimize losses. Usually this involves an attempt to track down the computer that is hosting the phishing website and to have that website removed or traffic to the site blocked.[70] This can be a laborious and time-consuming process given that the appropriate internet service provider (ISP) must be found and convinced to act.[71] Markus Jakobsson and Steven Myers report rumours that where this approach has been found to be ineffective, some service providers have launched DoS attacks on the phishing sites in order to prevent potential victims (their clients) from accessing the phishing sites.[72]

As for advance fee fraud, the Artists Against 419 used to offer a variety of "bandwidth hogging" tools to be used in a "419 Flash Mob".[73] These flash mobs were "organized bandwidth" attacks against fraudulent sites—many people repeatedly visited the sites until the sites reached their bandwidth limit or their internet hosts noticed the traffic and shut down the sites. As Artists Against 419 says, "[t]he whole time these run on your machine, you are stealing bandwidth from the scammers."[74]

A key problem with responding either with DoS or bandwidth hogging is that most spammers and phishers are using a network of compromised computers. As a result, an attempt to strike back at them will likely affect the owners of compromised computers and their ISPs rather than the criminals who easily move on to other compromised computers.

DoS or bandwidth hogging are also used to combat P2P file sharing of copyrighted works. MediaDefender is a company that offers "peer-2-peer anti-piracy solutions" of various types, including planting false files on

---

69 Phishing scams usually begin with a spam email constructed to look like a legitimate communication from, for example, a financial institution. The email invites the recipient to open a link to a spoof website, designed to look like the relevant institution's legitimate site, but is actually under the phisher's control. The recipient enters personal information, such as account details. The phisher collects this information and sells it to "cashiers" who make fraudulent use of it. The spoof website is often hosted on a computer that has previously been compromised through a security vulnerability or malware infection.

70 See Markus Jakobsson & Steven Myers, eds, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Hoboken, NJ: John Wiley & Sons, 2007) at 23.

71 See *ibid.*

72 *Ibid.*

73 "AA419 Tools", online: Artists Against 419 <http://wiki.aa419.org/index.php/AA419_Tools>.

74 *Ibid* at "Bandwidth Attack".

P2P networks to make finding a desired file more difficult and frustrating.[75] In addition, however, MediaDefender is also reported to use "interdiction" and "swarming".[76] Interdiction is a form of DoS, in which MediaDefender makes constant connections to the infringing files in order to exhaust the provider's bandwidth and to stop others from downloading the files.[77] Swarming is used to disrupt BitTorrent networks, which assemble files from small pieces gathered from different users. MediaDefender provides pieces containing the wrong data, so that the reassembled file is degraded.[78]

A recent controversy erupted when MediaDefender disabled the computer network of Revision3, a company that produces and distributes television shows via BitTorrent.[79] Revision3 had been running an open BitTorrent tracker (a server that coordinates communication between peers in the network who are trying to transfer files), which, unbeknownst to Revision3, was being used to list pointers to a large amount of unapproved copyrighted content.[80] MediaDefender had been accessing the tracker to post fake files, but when Revision3 noted the problem and closed the tracker over a holiday weekend in order to fix the problem, MediaDefender appears to have launched a DoS attack against the tracker. The attack shut down the company's Internet site, RSS server and internal email.[81] MediaDefender maintained this had never happened before and was unintentional, although Revision3, relying on other reports of MediaDefender's use of DoS, claimed that MediaDefender's servers were automatically programmed to launch DoS attacks on formerly open BitTorrent trackers that shut MediaDefender out. The CEO wrote a blog posting warning others of the risks of such mistakes:

> [W]hat if MediaDefender discovers a tracker inside a hospital, fire department or 911 center? If it happened to us, it could happen to them too. In my opinion, MediaDefender practices risky business, and needs to overhaul how it operates. Because in this country, as far as I know, we're still innocent until proven guilty—not drawn,

---

75 See Nate Anderson, "Peer-to-Peer Poisoners: A Tour of MediaDefender" (18 March 2007) at 3, online: Ars Technica <http://www.mediadefender.com/news/20070318_ARSTechnica.pdf> .

76 *Ibid.*

77 See *ibid.*

78 See *ibid.*

79 See David Kravets, "MediaDefender Defends Revision3 SYN Attack", Blog, *Wired* (31 May 2008), online: <http://blog.wired.com/27bstroke6/2008/05/mediadefender-d.html>; Joseph Menn, "Anti-piracy Misfire Takes Down Online TV Network" *Los Angeles Times* (30 May 2008), online: <http://articles.latimes.com/2008/may/30/business/fi-outage30>.

80 See Kravets, *supra* note 79.

81 See *ibid.*

> quartered and executed simply because someone thinks you're an outlaw.[82]

These anecdotes illustrate that DoS or at least bandwidth hogging have been used as a form of self-help in several instances in order combat spam, online fraud, and copyright infringement. These examples also illustrate some of the problems associated with self-help, namely, the risk of erroneously hitting an innocent party, as well as the risk of escalating conflicts as a cycle of response and counter-response develops.

2. Counterstrikes, Malware, and Hacking

There have been multiple suggestions in recent years that various forms of Internet counterstrikes ought to be permissible. The following overview illustrates the continuing interest in allowing people to hack back against those who are harming them online, as well as the continuing concern about the potential consequences of doing so.

In 2002, Timothy Mullen set off a lively debate over the propriety of Internet counterstrikes in the context of trying to stop the propagation of Internet worms. He proposed that it ought to be permissible to hack into computers infected with the Nimda worm in order to disable the worm and prevent its further propagation.[83]

In 2001, lobbyists attempted to have a provision included in the *USA Patriot Act*[84] that would have immunized copyright owners from liability for data losses they caused to others while attempting to "impede or prevent" electronic piracy.[85] These efforts culminated in the *Berman Bill* in

---

[82] Jim Louderback, "Inside the Attack that Crippled Revision3" Blog, *Revision3* (29 May 2008), online: <http://revision3.com/blog/2008/05/29/inside-the-attack-that-crippled-revision3/>.

[83] Timothy M Mullen, "Defending Your Right to Defend: Considerations of an Automated Strike-Back Technology" *Hammer of God* (10 September 2002), online: <http://www.hammerofgod.com/strikeback.txt>. Mullen writes that

> [w]e could certainly have attempted to remove the worms, or even patch the original vector that the worm used to infect the system, but we believe that is too much. We are not without respect for the property of the owners of the infected systems—we just (rightfully) value our own property more. To that degree, we want to cause the least possible alteration to the attacking system, and to leave it as close to its original configuration as possible. We want to adhere not only to the concept of "reasonable force," but to utilize "minimal force" where at all possible. Our goal is not to "fix" everyone's systems, and not to teach lax administrators a lesson. Our goal is to stop the propagation of global worms (*ibid*).

[84] Pub L No 107-56, 116 Stat 272 (2001).

[85] Declan McCullagh, "RIAA Wants to Hack Your PC" *Wired* (15 October 2001), online: <http://www.wired.com/politics/law/news/2001/10/47552> [McCullagh, "Hack Your PC"].

2002, which would have provided legal immunity for disabling P2P file-sharing networks where there was a "reasonable basis" to believe piracy was occurring.[86] The bill was criticized on the ground that it would permit content owners to shut down networks with impunity, affecting all activity and not just piracy.[87] In 2003, Senator Orrin Hatch expressed support for the idea of aggressive counterstrikes against copyright infringers at a Senate Judiciary Committee hearing on copyright infringement. "If we can find some way to do this without destroying their machines, we'd be interested in hearing about that ... If that's the only way, then I'm all for destroying their machines."[88] In 2004, Symbiot released a whitepaper arguing in favour of "active countermeasures" in defence of computer systems[89] and announced a new computer security service that involved a range of aggressive countermeasures, apparently including "disabling, destroying, or seizing control over the attacking assets."[90] The whitepaper defended the use of offensive tactics, including DDoS, "special operations experts applying invasive techniques", and "psychological operations".[91] The possibility that these approaches would be used generated considerable concern in the security community.[92] The descriptions were somewhat vague and no longer seem to be available from Symbiot.

---

86 US, Bill HR 5211, *To Amend Title 17, United States Code: To Limit the Liability of Copyright Owners for Protecting Their Works on Peer-to-Peer Networks*, 107th Cong, 2002, online: US Government Printing Office <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h5211ih.txt.pdf>. See also Declan McCullagh, "Hollywood Hacking Bill Hits House" *CNET News* (25 July 2002), online: <http://news.cnet.com/2100-1023-946316.html> [*Berman Bill*]; Howard Berman, "Introduction of the Peer to Peer Piracy Prevention Act" (Statement delivered at the United States House of Representatives, Washington, DC, 25 July 2002), online: <http://www.house.gov/list/press/ca28_berman/piracy_prevention_act.shtml>.

87 See McCullagh, "Hack Your PC", *supra* note 85.

88 "Senator Takes Aim at Illegal Downloads," *USA Today* (19 June 2003), online: <http://www.usatoday.com/tech/news/techpolicy/2003-06-18-hatch-wants-computers-dead_x.htm>.

89 Paco X Nathan & Mike W Erwin, White Paper, 78766-9646, "On the Rules of Engagement for Information Warfare" (4 March 2004), online : Symbiot <http://www.symbiot.com/pdf/iwROE.pdf>.

90 Bruce P Smith, "Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help" (2005) 1:1 Journal of Law, Economics and Policy 171 at 177-78 [footnotes omitted]; See also Bootie Cosgrove-Mather, "Vigilante Justice in Cyberspace" *CBS News* (21 June 2004), online: <http://www.cbsnews.com/stories/2004/06/21/tech/main625144.shtml>.

91 Nathan & Erwin, *supra* note 89.

92 See e.g. Sharon Gaudin, "Plan to Fight Back Against Hackers Causes Stir," *ESecurityPlanet* (17 March 2004), online: <http://www.esecurityplanet.com/prodser/article.php/3327391/Plan-to-Fight-Back-Against-Hackers-Causes-Stir.htm>; Smith, *supra* note 90

The exploration by two lawyers of the possibility of having courts approve the hacking of counterfeiters' websites, after attempts to pursue the websites through ISPs had been exhausted, raised considerable criticism in 2005.[93] The concerns had to do chiefly with the risk of harm to innocent third parties, concern over the possible abuse of power, and the escalation of the technological battle between the counterfeiter and the court-sanctioned hacker.[94]

Some groups and individuals strike back against phishing sites by hacking into them and modifying them to reveal that they are fraudulent sites.[95] In the words of one of the groups doing this, "[l]aw enforcement cannot be bothered with them—but we can!"[96]

The Internet counterstrikes that may be launched vary from relatively passive to quite aggressive, and these attacks may differ widely in the degree of unintended damage they are able to cause.[97] One key concern is that many cybercrimes are perpetrated using compromised computers, the owners and administrators of which may be unaware that their computers are being used in this way. In addition, attackers may use false source addresses, meaning that a counterstrike may hit an innocent party, perhaps generating an escalating battle when the innocent parties themselves react to what—to them—is an unprovoked attack.[98] Several legal scholars have considered Internet counterstrikes, suggesting that they be permitted in limited circumstances, but only when accompanied with a responsibility to pay damages where the attack is mistakenly

---

at 179; Munir Kotadia, "Security Product to Strike Back at Hackers," *CNET News* (10 March 2004), online: <http://news.cnet.com/2100-7349_3-5172032.html>.

93 See Ronald D Coleman, "Lawyerhacking Defended: Co-author of Copyright Hacking Article Replies to Politech" *Politech* (24 October 2005), online: <http://www.politechbot.com/2005/10/24/author-of-copyright/>.

94 See Declan McCullagh, "More on Barney Lawyer Yearning to Hack Copyright Infringers' Sites" *Politech* (18 October 2005), online: <http://www.politechbot.com/2005/10/19/more-on-barney/>.

95 See "Vigilantes Deface Phishing Sites" *Sydney Morning Herald* (26 May 2005), online: <http://www.smh.com.au/news/Breaking/Vigilantes-defacing-phishing-sites/2005/05/26/1116950789334.html>.

96 *Ibid.*

97 For methods to distinguish between attackers and innocent users before taking action against them, see Haroon Meer, Roelof Temmingh & Charl Van der Walt, "When the Tables Turn: Passive Strike-Back" in Neil R Wyler, ed, *Aggressive Network Self-Defense* (Rockland, MA: Syngress, 2005) 339 at 358.

98 See Jayaswal, Yurcik & Doss, *supra* note 64 at 383; Orin S Kerr, "Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability," (2005) 1:1 Journal of Law, Economics and Policy 197.

launched against a legitimate party or where innocent bystanders are harmed.[99]

In addition to the counterstrikes discussed above, there are other illegal methods that may be used to combat online fraud and crime. Malware (including viruses, worms, and Trojans) may be used in attempts to gather evidence of cybercrime. For example, one amateur detective loaded a Trojan horse program masquerading as a photograph onto child pornography sites in order to infect the computers of users of those sites. The information about child pornography found on those computers was subsequently passed to police.[100] Information obtained in this way has led to convictions on several occasions, although there is a risk that evidence of this type may be excluded as unconstitutional.[101]

Malware has also been used to try to combat the spread of Internet worms.[102] In the aftermath of the MSBlast worm epidemic, unknown parties wrote another worm, which scanned the Internet for computers with the same vulnerability as that exploited by MSBlast and then installed a patch to protect the vulnerable systems against it.[103] Although the intentions were good, the spread of the remedial worm, known as Welchia or Nachi, overwhelmed some networks. In fact, Air Canada's computer systems were affected, resulting in flight delays and cancellations.[104]

3. Data Poisoning

One of the responses that appears to have developed to deal both with phishing and with copyright infringement is the technique known as "di-

---

99 See e.g. Lichtman, *supra* note 51 at 254; Smith, *supra* note 90 at 175.

100 See Nancy Gohring, "Digital Vigilantes: Hacking for a Good Cause" *PCWorld* (26 December 2007), online: <http://www.pcworld.com/article/140731/digital_vigilantes_ hacking_for_a_good_cause.html>.

101 See *United States v Steiger*, 318 F 3(d) 1039, 16 Fla L Weekly Fed C 197 (11th Cir 2003); *United States v Jarrett*, 338 F 3(d) 339, 61 Fed R Evid Serv 1530 (4th Cir 2003) rev'g 229 F Supp 2(d) 503 (ED Va 2002); Lisa M Bowman, "Judges OK Evidence from Hacker Vigilante," *CNET News* (1 August 2001), online: <http://news.cnet.com/Judges-OK-evidence-from-hacker-vigilante/2100-1029_3-5058835.html>; Sharon Gaudin, "Vigilante Hacker's Evidence Puts Judge Behind Bars" *Information Week* (23 February 2007), online: <http://www.informationweek.com/news/security/showArticle.jhtml?articleID=197008431>.

102 See Ingrid Marson, "Anti-Santy Worm on the Prowl" *CNET News* (31 December 2004), online: <http://news.cnet.com/Anti-Santy-worm-on-the-prowl/2100-7349_3-5508607.html>. Curtis EA Karnow "Launch on Warning: Aggressive Defense of Computer Systems" (2004) 7 Yale JL & Tech 87 at 93 (discussing the creation of anti-Code Red II malware).

103 See Robert Lemos, "'Good' Worm, New Bug Mean Double Trouble," *CNET News* (19 August 2003), online: <http://news.cnet.com/2100-1002_3-5065644.html>.

104 See *ibid.*

lution", "data poisoning", or "decoy files". In essence, this involves the delivery of a large quantity of false information or degraded files to a site or network in order to reduce the overall usefulness of the data available there. The boundary between dilution and DoS attacks becomes blurred where the amount of disinformation supplied to the targeted site overwhelms that site.[105] Dilution also can be legally questionable where it violates the contractual terms of use of a targeted site.

There are multiple examples of the dilution approach to self-help in the context of fighting spam, phishing, and file sharing. Dilution was tried very early on in the battle against spam. Spammers use bots to harvest email addresses by crawling through websites. One early approach to fighting spam was to try to poison the spammers' email address lists by creating enticing pages full of false email addresses, with links to an endless loop of further pages of false email addresses.[106]

In the context of phishing, some banks are reported to have responded by submitting large amounts of false financial information in order to dilute the useful information being received by the phisher.[107] Some anti-phishing service providers offer dilution, which involves feeding false credentials to phishing websites.[108] MarkMonitor writes that "[w]hen appropriate, MarkMonitor injects active phish sites with properly-formatted—but fake—credentials, rendering them virtually harmless."[109] Other volunteer organizations have adopted other forms of poisoning to combat phishing. Artists Against 419 offers a "Fake Bank Form Filler", which automates the process of filling in false bank information on phishing pages.[110] Phishfighting.com invited people to send them the URLs included in phishing emails. It would then submit thousands of false entries

---

[105] See Alice Dragoon, Sarah D Scalet & Bob Violino, "Phishing: the Basics" *CSO Security & Risk* (April 2009), online: <http://www.csoonline.com/article/221737/Phishing_The_Basics>.

[106] See James Glave, "Wpoison Sets Trap for Spam Weasel," *Wired* (2 December 1997), online: <http://www.wired.com/science/discoveries/news/1997/12/8852>. For a discussion of Wpoison, see "Wpoison", online: Infinite Monkeys & Company <http://www.monkeys.com/wpoison/>. For a listing of various bot poisoning programs, see "Poisoning Spambots" (2 May 2008), online: <http://spamlinks.net/prevent-spambots-poison.htm>.

[107] See Brian Krebs, "New Industry Helping Banks Fight Back" *The Washington Post* (4 March 2005), online: <http://www.washingtonpost.com/wp-dyn/articles/A6367-2005Mar4.html>.

[108] See Munir Kotadia, "Fighting Fraud by Baiting Phishers" *CNET News* (31 March 2006), online: <http://news.cnet.com/Fighting-fraud-by-baiting-phishers/2100-1029_3-6056317.html>.

[109] "Anti-Fraud Solutions", online: Mark Monitor <http://www.markmonitor.com/products/antifraud-solutions.php>.

[110] See Artists Against 419, *supra* note 73 at "Refi Retaliator II—Fake Bank Form Filler".

to the phishing sites. Phishfighting.com avoided the DoS effect by submitting its entries once every twenty seconds, which would not be enough to consume the phisher's bandwidth.[111] The dilution or poisoning approach may not provide a serious impediment to phishers who may simply automate the verification of the data they collect, or devise methods to detect submissions from suspicious sources (e.g., multiple submissions from one source, or submissions sent via anonymous remailers and cloakers).[112]

The dilution approach has also been adopted by copyright owners to combat P2P file sharing. The method involves injecting into the network large numbers of decoy files that look like the desired files but in fact are unreadable or different from what was expected.[113] This is meant to discourage file sharing by making it harder for people to find the files they wish to download. As a result, P2P systems have developed techniques to defeat poisoning, including various forms of reputation system.[114]

MediaDefender is a company that offers "peer-2-peer anti-piracy solutions," which are described as "*non-invasive technological countermeasures* ... to frustrate users' attempts to steal/trade copyrighted content."[115] The company states that "decoying" and "spoofing" are their most commonly used techniques, which involve planting false files in P2P networks and sending searchers to the wrong locations in order to make the real file more difficult and frustrating to locate.[116]

---

[111] "How PhishFighting works" (1 September 2005), online: Phishfighting.com <http://web.archive.org/web/20080616015452/www.phishfighting.com/FAQ.aspx?anti_spyware>.

[112] See Sandi Hardmeier, "Fighting Back Against Phishing—Two Wrongs do not Make a Right", Blog, *Spyware Sucks* (11 September 2005), online: <http://msmvps.com/blogs/spywaresucks/archive/2005/09/11/66113.aspx>.

[113] See Nicolas Christin, Andreas S Weigend & John Chuang, "Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks" (2005) [unpublished, archived at ACM], online: p2pecon@berkeley <http://p2pecon.berkeley.edu/pub/CWC-EC05.pdf>.

[114] See *ibid* at 7. For a discussion of IP blocking programs "to significantly reduce your chances of connecting with malicious peers", see e.g. "IP Blocking for uTorrent in Windows XP & Vista" (1 April 2008), online: FileShareFreak <http://filesharefreak.com/tag/ip-blocking/>. The Bluetack blocklist FAQ indicates that users of P2P should use at least Level 1 blocking, which blocks *inter alia* companies known to be involved with trying to stop file sharing, companies that have a strong financial interest in copyrighted material, and a range of others from whom "anti-P2P activity has been observed." See "FAQ Questions about the Blocklists: What is in the blocklists?", online: Bluetack Internet Security Solutions <http://www.bluetack.co.uk/forums/index.php?autocom=faq&CODE=02&qid=17>.

[115] "Peer-2-Peer Anti-Piracy Solutions" (2007), online: MediaDefender <http://www.mediadefender.com/antipiracy.html> [emphasis in original].

[116] See Anderson, *supra* note 75 at S3.

One of the standard license terms included in the P2P software program KaZaA forbids users from intentionally uploading "spoofed files or files with information designed to misidentify the actual content of the file."[117] Although some suggest that this provision might be void as contrary to public policy, the provision technically does make poisoning a breach of contract.[118]

4. Defamation Attacks

Defamation attacks are attempts to disrupt the underground marketplaces in which stolen financial information is traded.[119] These sophisticated online marketplaces feature volume discounts, and pricing variations, such as higher pricing for stolen credit cards with higher credit limits.[120] Also available on these markets are bank account data and "full identities [including] date of birth, address, and social security and telephone numbers."[121] Administrators of the markets verify participants in an attempt to permit market participants to distinguish between the "honest" and "dishonest" criminals.[122] Various services are also advertised, including those of cashiers who specialize in converting financial data into money, and others who sell the email lists and compromised computers for use in phishing.[123]

---

[117] "KaZaA End User License Agreements" at s 2.15, online: KaZaA <http://www.kazaa.com/us/eula.htm#kazaa_eula> cited in Lichtman, *supra* note 51 at 253 ("2.15 Intentionally make available 'spoofed' files or data, or files or data with any type of information designed to misidentify the actual content of a file or which is intended to mislead the recipient of the file").

[118] See Lichtman, *supra* note 51 at 253-54.

[119] See John Dunn, "Supermarket for Stolen Credit Cards Found" *Techworld* (26 March 2008), online: <http://www.techworld.com/security/news/index.cfm?newsid=11808>; Tom Zeller Jr, "Black Market in Stolen Credit Card Data Thrives on Internet" *The New York Times* (21 June 2005), online: <http://www.nytimes.com/2005/06/21/technology/21data.html>; Dean Turner, ed, White Paper, "Symantec Global Internet Security Threat Report: Trends for July–December 07", vol 8, (Symantec, 2008) at 17, online: Symantec <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pfd>.

[120] See *ibid* at 19.

[121] Jacob Leibenluft, "Credit Card Numbers for Sale: How Much Does a Visa or MasterCard Number Go For these Days?", *Slate* (24 April 2008), online: <http://www.slate.com/id/2189902/>.

[122] See Jason Franklin et al, "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants" (Paper presented to the 14th ACM Conference on Computer and Communications Security, Alexandria, Va, 29 October- 2 November 2007) [unpublished] at 376, online: The International Computer Science Institute Networking Group <http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf>.

[123] See *ibid* at 376.

Researchers of these underground marketplaces have suggested a couple of counter-measures to reduce the number of transactions.[124] The so-called "slander attack" involves eliminating the verified status of a buyer or seller through "false defamation."[125] The purpose is to create a lemon market by falsely defaming verified participants, so that there is no price advantage to trustworthiness, causing the general quality of the market to decline.[126]

Although it seems unlikely that the victims would complain, it may be defamatory to spread false information that a vendor of stolen credit cards sells cards that will not work. It is generally defamatory to impute dishonesty to someone, although in this case it seems inappropriate for the law to protect a reputation for "honour among thieves".

C. Application of the Principles to Self-Help in Cyberspace

The purpose of this section is to illustrate how the principles of technological self-help, discussed above, might play out in the context of some of these types of self-help in cyberspace. In particular, I will consider the effects on equality of the use of the Internet in these self-help activities, the issue of arms racing, and the problem of harm to bystanders.

Inequality in physical strength is not the relevant dimension of inequality in the context of online attacks. Instead, attackers and victims may differ in the degree of computing expertise or the amount of bandwidth that they can muster. In addition, cyberspace has several structural attributes that more subtly affect the balance of strength between parties online. I will call two of these attributes the "amplification effect" and the "coordination effect".

One key attribute of the Internet is the amplification effect. In essence, the Internet enables one person to affect a huge number of people since it both shrinks distances and permits a high degree of automation. The collapse of distances allows an individual on one side of the globe to consider hacking targets throughout the world. Automation renders activities like spamming and phishing profitable because of the scale increase and cost reduction that it enables. It is fair to say that this attribute of the Internet amplifies the power and reach of the individual.

The coordination effect is another key attribute of the Internet. It flows from the "many-to-many" structure of the network. In essence, col-

---

[124] See *ibid.*

[125] *Ibid* at 387.

[126] See *ibid.*

laboration between large and physically scattered groups of people is made simple. Examples of this effect are numerous: wikis and P2P file sharing are two such examples. DDoS attacks also illustrate this effect. The flood of communications that disable a target is made possible by harnessing an army of individual computers into a coordinated attack. In these examples, individual people or computers are empowered by the network to accomplish things collectively that simply could not be done as effectively alone.

All of these factors suggest that the Internet has shifted power toward individuals, for better or worse, considerably beyond their previous limitations. In some cases, this power is misused against others online. An approach to self-help that is sensitive to inequality would permit victims to adopt measures that are arguably necessary to neutralize the level of strength that an attacker obtains through the amplification and coordination effects, as well as through a higher-than-usual level of technical know-how. This would mean (a) permitting victims to employ security services to defend themselves, in order to neutralize the disparity in technical know-how between victims and attackers; (b) permitting victims to make use of the coordination effect by engaging in certain forms of collective response (e.g., bandwidth-hogging tools up to and perhaps including DDoS attacks); (c) permitting victims to disrupt the harmful use of coordination by others (e.g., by permitting defamation attacks and by allowing data poisoning of file-sharing networks with degraded and mislabeled versions of copyrighted content); and (d) permitting victims to take advantage of the amplification effect (e.g., bandwidth hogging up to and perhaps including levels of DoS).

As is the case with self-help in general, where a victim fights back in a manner that is unreasonably dangerous, bystanders who are harmed may sue in negligence. This is most likely a necessary control on the use of self-help in cyberspace, where it is likely that bystanders may be harmed by certain kinds of attacks. As noted above, many forms of harmful activity online are launched from networks of compromised computers—"botnets". On the one hand, an attack on one of these computers is unlikely to greatly disrupt the activities of the controller of the botnet, since the botnet offers thousands of compromised computers to take the place of the attacked computer. On the other hand, the hapless owner of that computer and his ISP will have to deal with the attack. Where a victim attacks a phishing website hosted on a compromised computer, the ISP who offers services for that computer and other users of the ISP's services will have their service degraded as well. The existence of a claim in negligence for such cases would hopefully ensure that the risk being imposed by the party engaging in self-help was reasonable under the circumstances, and that the harm to innocent bystanders was not too severe.

In fact, an approach of this type might spur innovation in the area of how to target responses more carefully. For example, Meer, Temmingh, and Van der Walt propose an intermediate response that they call "passive strike-back". They suggest that the danger of harming innocent parties is obviated with the passive strike back because

> [t]he driving principle behind passive strike-back is that the strike-back is never 'launched' against anyone. Unlike signature-based defence systems passive strike-back doesn't attempt to spot an attack and then respond, rather passive strike-back allows the attacker to 'fetch' the strike-back attack himself.[127]

As they say, "[i]f we can accurately distinguish an attacker who surfs our site from a legitimate user, we can easily send malicious code to be executed in the browser."[128] They suggest mechanisms to distinguish attackers from legitimate users, such as responding to scanners with intriguing messages that suggest vulnerability at a particular location and delivering malicious code only to those who then go to the location to investigate.[129]

Clearly, innovation of this type is likely to draw forth counter-innovation in how to dodge these techniques. It is the kind of technological arms race that legal regulation is sometimes required to halt. The question is whether technological self-help is in fact a wasteful arms race that we wish to stop. Unlike the invention of bigger and more destructive weapons with which to out-class an opponent, the kind of invention in this arms race may involve techniques more akin to cloaking, detection, counter-cloaking, and so on. This type of arms race may generate innovations with other uses and so might not be a wasteful arms race.

In sum, a concern with inequality of strength in the context of cyberspace attacks would look not at physical strength but at the manner in which the Internet provides an attacker with the ability to launch automated and coordinated attacks across great distances. It would suggest that a defender should be able to make use of technological responses that help neutralize this disparity in strength. Yet, the problem of harm to bystanders is a real one, which should be controlled through negligence liability. This liability risk may help generate useful innovation in the form of techniques that offer a more precisely targeted and calibrated response that reduces harm to bystanders.

---

127 Meer, Temmingh & Van der Walt, *supra* note 97 at 351.

128 *Ibid* at 358.

129 See *ibid.*

Conclusion

This article has sought to clarify the relationship between legal self-help, technology, and equality. Each of these three elements is in a complex relationship with the other two.

With respect to self-help and technology, the legal rules guiding self-help sometimes condone and sometimes prohibit resort to technological tools with which to pursue one's legal interests. This has important ramifications for the efficacy of self-help. Technological evolution may challenge the balance at the heart of the rules on self-help. Technologies may increase or decrease destructiveness and risks to bystanders. In addition, if technologies can be freely used to pursue legal interests, a technological arms race may develop. It is necessary to consider whether that arms race is wasteful or productive when deciding whether or not resort to a given technology should be an acceptable action in self-help.

Self-help regimes and equality are also linked. Self-help regimes are said to undermine equality since they favour the strong over the weak, which suggests that a monopoly on state enforcement of legal rights is more conducive to social equality. This is not necessarily true, given that access to justice is not equally distributed.

As for the relationship between technology and equality, the usual story of the source of inequality, rooted in unequal access to technology, is an incomplete picture. Technologies may promote or decrease equality, and may do so to a net social benefit or detriment. Some technologies may require us to face a difficult choice between allowing the use of technologies that promote equality and imposing net social costs on other values.

In the end, the principles for determining the legal bounds of technological self-help should build on the recognized self-help principles related to necessity, reasonableness, and proportionality. When determining whether to accept the use of a given technology, the principles should also include explicit consideration of the effects on equality, the bystander risks, and the question of whether the innovative arms race would be wasteful or productive.

The forms of human interaction and the nature of the harms that matter, shift with technological evolution. Therefore, when considering the effects of a technology on equality when used in self-help, one should consider not only equality in physical strength—the usual dimension of equality at issue in self-defence, for example—but also other ways in which parties differ in their ability to protect their legal interests.