HACKTIVISM, ANONYMOUS & A NEW BREED OF PROTEST IN A NETWORKED WORLD

Noah C.N. Hampson

Introduction

Early on the morning of November 30, 2010, WikiLeaks.org came under assault by a hacker known as "th3j35t3r" (The Jester).[1] By launching what is known as a denial of service (DoS) attack with software of his own invention, The Jester overwhelmed WikiLeaks' servers with requests for information.[2] WikiLeaks.org soon crashed, and remained down for over a day.[3] Days before, WikiLeaks made international headlines by posting on its website roughly 250,000 classified documents stolen from the U.S. government.[4] On his Twitter feed, The Jester claimed credit: "www.wikileaks.org — TANGO DOWN — for attempting to endanger the lives of our troops, 'other assets' & foreign relations #wikileaks #fail".[5]

To get its web site back online, WikiLeaks promptly switched hosting providers and began renting bandwidth from Amazon.com.[6] DoS and other attacks against WikiLeaks continued, but were unsuccessful.[7] Shortly thereafter, however, Amazon ousted WikiLeaks from

---

[1] Sean-Paul Correll, *'Tis the Season of DDoS – WikiLeaks Edition*, PandaLabs Blog (Dec. 4, 2010), http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/.

[2] *See* Neil J. Rubenkind, *WikiLeaks Attack: Not the First by th3j35t3r*, PC (Nov. 29, 2010), http://www.pcmag.com/article2/0,2817,2373559,00.asp

[3] *See* Correll, *supra* note 1.

[4] *See* Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. Times, Nov. 29, 2010, at A1, *available at* http://www.nytimes.com/2010/11/29/world/29cables.html.

[5] *See* Lee, *Wikileaks and th3j35t3r – Has He Made the Right Call?*, Security FAQs Blog (Nov. 30, 2010), http://www.security-faqs.com/wikileaks-and-th3j35t3r-has-he-made-the-right-call.html.

[6] *See* Anahad O'Connor, *Amazon Removes WikiLeaks from Servers*, N.Y. Times (Dec. 2, 2010), *available at* http://www.nytimes.com/2010/12/02/world/02amazon.html?scp=1&sq=wikileaks%20&%20Amazon&st=cse.

[7] *See* Charlie Savage, *Amazon Cites Terms of Use in Expulsion of WikiLeaks*, N.Y. Times, Dec. 2, 2010, at A10, *available at*

its servers after Senator Joseph Lieberman contacted Amazon "for an explanation" of its decision to provide hosting services to the whistleblower site.[8] WikiLeaks then moved to another hosting service, but again was cut off by the service provider after ongoing DoS attacks threatened the stability of every other website hosted by the provider.[9] Finally, after establishing a number of mirror sites (thereby multiplying the number of sites on which the content of the WikiLeaks site appeared), the WikiLeaks web site was once again stable.[10]

The controversy surrounding WikiLeaks, however, was only beginning. Soon, major companies who had provided services to WikiLeaks and its users began withdrawing support.[11] Citing violations of its Acceptable Use Policy, PayPal cancelled WikiLeaks' account, preventing WikiLeaks from receiving donations through the popular online payment service.[12] Three days later, MasterCard suspended payments made to WikiLeaks by cardholders.[13] One day later, Visa did the same.[14] Swiss bank PostFinance closed the account of WikiLeaks founder Julian Assange, claiming that Assange had provided false in-

---

http://www.nytimes.com/2010/12/03/world/03amazon.html?scp=3&sq=wikileaks%20&%20Amazon&st=cse.

[8] *See* Steve Ragan, *Recap: WikiLeaks Faces More Heat in the Wake of Cablegate*, Tech Herald (Dec. 4, 2010), http://www.thetechherald.com/article.php/201048/6505/Recap-WikiLeaks-faces-more-heat-in-the-wake-of-cablegate; Press Release, Sen. Joseph Lieberman, Internet Company Had Hosted WikiLeaks Website (Dec. 1, 2010), http://lieberman.senate.gov/index.cfm/news-events/news/2010/12/amazon-severs-ties-with-wikileaks. *But see* Austin Carr, *Why Lieberman Had Nothing to Do with Amazon Dropping WikiLeaks*, Fast Company (Dec. 3, 2010), http://www.fastcompany.com/1707262/why-lieberman-had-nothing-to-do-with-amazon-dropping-wikileaks (quoting Lieberman's communications director as denying that the senator specifically asked Amazon to remove WikiLeaks).

[9] *See* Taylor Barnes, *Booted from US-Based Domain, WikiLeaks Site Finds Refuge with Swiss Pirate Party*, Christian Sci. Monitor (Dec. 3, 2010), http://www.csmonitor.com/World/terrorism-security/2010/1203/Booted-from-US-based-domain-WikiLeaks-site-finds-refuge-with-Swiss-Pirate-Party.

[10] *See* Ragan, *supra* note 8 (quoting EveryDNS.net's press release concerning WikiLeaks and providing a link to a list of WikiLeaks' mirror sites).

[11] *See id.*

[12] *See PayPal Statement Regarding WikiLeaks*, PayPal Blog (Dec. 3, 2010), https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/.

[13] *See* Declan McCullagh, *MasterCard Pulls Plug on WikiLeaks Payments*, CNET News (Dec. 6, 2010, 2:37 PM PST), http://news.cnet.com/8301-31921_3-20024776-281.html?tag=mncol;1n.

[14] *See Visa Suspends All Payments to WikiLeaks*, USA Today (Dec. 7, 2010, 10:12 AM), http://www.usatoday.com/money/industries/technology/2010-12-07-visa-wikileaks_N.htm.

formation concerning his place of residence.[15] Bank of America, citing concerns that WikiLeaks "may be engaged in activities that are, among other things, inconsistent with our internal policies," likewise pulled the plug, refusing to process payments to WikiLeaks.[16]

The uproar that accompanied this news sparked an online backlash.[17] An amorphous group of individuals from around the world, known collectively as "Anonymous," began to bombard the websites of the companies and other entities the group deemed opposed to WikiLeaks with distributed denial of service (DDoS) attacks, causing many of the sites to crash, and rendering others inoperable for some time.[18] The group's mission, called "Operation Payback," was to raise awareness of the actions of the groups opposed to WikiLeaks; fight what it perceived as censorship by identifying those responsible for the attacks on WikiLeaks and attacking them in return; and support "those who are helping lead our world to freedom and democracy."[19]

To some, the conflict surrounding the WikiLeaks controversy was the first real example of a war over digital information.[20] John Perry Barlow, co-founder of the Electronic Frontier Foundation, announced that "[t]he first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops."[21] To others, including members of the group itself, "Operation Payback" is merely the most prominent recent example of a trend that has been developing since the invention of the Internet: computer-savvy individuals deploying their skills online to protest for or against a cause—or, more simply, "hacktivism."[22]

---

[15] *See* Matthew Allen, *Former WikiLeaks "Bank" Still Denied License*, SWISSINFO.CH (Dec. 21, 2010, 3:38 PM), http://www.swissinfo.ch/eng/business/Former_WikiLeaks_bank_still_denied_licence.html?cid=29080126.

[16] *See* Steven Musil, *Bank of America Cuts off WikiLeaks*, CNET NEWS (Dec. 18, 2010, 8:24 AM PST), http://news.cnet.com/8301-31921_3-20026103-281.html?tag=mncol;5n.

[17] *See* Sean-Paul Correll, *Operation: Payback Broadens to "Operation Avenge Assange"*, PANDALABS BLOG (Dec. 6, 2010), http://pandalabs.pandasecurity.com/operationpayback-broadens-to-operation-avenge-assange/.

[18] *See id.*

[19] *See id.*

[20] *See* Raphael G. Satter & Peter Svensson, *WikiLeaks Fights to Stay Online amid Attacks*, BLOOMBERG BUSINESSWEEK (Dec. 3, 2010, 11:27 AM ET), http://www.businessweek.com/ap/financialnews/D9JSHKUG0.htm.

[21] *See id.*

[22] *See* Noa Bar-Yosef, *How Operation Payback and Hacktivism are Rocking the 'Net*, SECURITYWEEK (Dec. 15, 2010), http://www.securityweek.com/how-operation-payback-and-hacktivism-are-rocking-net; Jan-Keno Janssen et al., *Operation Payback: Protests via Mouse Click*, THE H SECURITY (Dec. 9, 2010, 9:35 PM), http://www.h-

Given that hacktivism is, like many aspects of Internet activity, transnational in scope, it is widely accepted that any effective legal response will require some degree of international cooperation.[23] Part I of this Note describes the differences between hacking and hacktivism. In addition to investigating the threats posed by hackers, this section explores the desirable aspects of hacktivism. Part II discusses the existing international legal framework in the area of cybersecurity, in particular the Council of Europe's Convention on Cybercrime. It also compares the domestic regimes of criminal laws affecting hacktivism in two key signatory states, the United States and the United Kingdom. Part III analyzes how certain methods of hacktivism may be compared to conventional means of protest. Finally, this Note concludes that a narrow subset of hacktivism is sufficiently similar to traditional forms of demonstration so as to warrant protection as a legitimate form of protest.

I. Background

A. *A Brief Description of Hacktivism*

The term "hacktivism" has been defined as the nonviolent use for political ends of "illegal or legally ambiguous digital tools" like web site defacements, information theft, web site parodies, denial-of-service attacks, virtual sit-ins and virtual sabotage.[24] Capitalizing on the power and pervasiveness of the Internet, hacktivists attempt to exploit its manifold access points to gain publicity and spread information about their views.[25]

---

online.com/security/news/item/Operation-Payback-protests-via-mouse-click-1150790.html.

[23] *See* Nat'l Security Council, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (2010), at iv, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; Daniel E. Geer, Jr., *Cybersecurity and National Policy*, 1 Harv. Nat'l Sec. J. i, ix (2010); Jessica L. McCurdy, *Computer Crimes*, 47 Am. Crim. L. Rev. 287, 326 (2010).

[24] *See* Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation (Sept. 2004) iii (unpublished Ph.D. dissertation, Harvard University), *available at* http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf. Samuels' work gives a thorough analysis of hacktivism from an empirical political science perspective. *See generally id.*

[25] *See id.* at 5 (quoting Pippa Norris, Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide (2001)).

Although it has not always carried a clever name, people have turned to hacktivism since the Internet's early days.[26] For example, to protest the passage of the Communications Decency Act of 1996, a hacker defaced the web site of the Department of Justice (DOJ) with images and commentary:

> Free speech in the land of the free? Arms in the home of the brave? Privacy in a state of wiretaps and government intrusion? Unreasonable searches? We are a little behind our 1984 deadline, but working slowly one amendment at a time. It is hard to trick hundreds of millions of people out of their freedoms, but we should be complete within a decade.[27]

Furthermore, as the behavior of The Jester and Anonymous demonstrate, hacktivism is often used by all sides in a debate.[28]

As the Internet has evolved, so too have the tools used by hacktivists to pursue their ideological objectives, and an individual's objective and point of view will likely determine his form of hacktivism.[29] Forms of hacktivism run the gamut from those that are clearly covered by existing anti-hacking laws—like redirects, site defacements, sabotage, and DoS attacks[30]—to forms whose legality is far less certain, like virtual sit-ins and site parodies.[31]

B. *Hacktivism vs. Hacking*

Hacktivism has origins in both hacking and activism;[32] however, distinguishing between hacktivism and hacking is not straightforward.[33] In one sense, the two have divergent motives.[34] But the term "hacking" has not always been used to describe the conduct of a cybercriminal.[35] It originally described an innovative use of technology

---

[26] *See id.* at 9; Bar-Yosef, *supra* note 22.

[27] Samuel, *supra* note 24, at 9 (citing copy of site defacement stored on mirror site unavailable to public).

[28] *Compare* Lee, *supra* note 5 (analyzing th3j35t3r's attacks on WikiLeaks), *with* Correll, *supra* note 17 (analyzing conduct of members of Anonymous in response to WikiLeaks controversy).

[29] *See* Samuel, *supra* note 24**Error! Bookmark not defined.** at 8, 48–49.

[30] *See id.* at 49.

[31] *See id.* at 71, 72.

[32] *See id.* at iii.

[33] *See id.* at 39.

[34] *See id.* at 4.

[35] *See* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 39–44.

to solve a problem.[36] In addition, hacking is frequently practiced in defense or furtherance of a unique set of norms that have developed as part of the culture of the Internet.[37] For present purposes, however, hacking may be differentiated from hacktivism by a lack of political objectives.[38]

Much hacking is motivated by nefarious and fraudulent aims.[39] Hackers are responsible for identity theft, fraud, commercial espionage, and other crimes with an annual cost in the trillions of dollars.[40] The FBI has declared that cybercrime is the most significant criminal threat, and that anti-cybercrime efforts are a top priority, behind only counterterrorism and counterintelligence.[41]

Moreover, cyberwarfare, waged by hackers on behalf of state and non-state actors, is considered the next phase in the evolution of threats to national security.[42] As such, this species of hacking arguably is motivated by political objectives; a major difference from hacktivism, however, is that hacking in cyberwarfare may be analogized to operations on the battlefront, while some forms of hacktivism may be compared to sit-ins or other forms of civil disobedience.[43] Mike McConnell, former director of national intelligence, told President Bush in 2007 that if the perpetrators of the September 11th attacks had instead successfully targeted a single American bank with cyber-attacks, the damage to the U.S. economy would have been "an order-of-magnitude" greater.[44] Similarly, law enforcement officials fear that cyber-attacks on the networks on which the nation's critical infrastructure is dependent—e.g., air traffic control systems, electrical grids,

---

[36] *See id.* at 51.

[37] *See id.* at 39.

[38] *But see id.* at 42 (noting that while on its face hacking may seem apolitical, there are certain inherently political aspects of hacker culture).

[39] *See id.* at 4; Steven R. Chabinsky, Deputy Assistant Dir., Cyber Div., FBI, Address at the GovSec/FOSE Conference, Washington D.C.: The Cyber Threat: Who's Doing What to Whom (Mar. 23, 2010) (transcript *available at* http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom).

[40] *See* Will Knight, *Hacking Will Cost World $1.6 Trillion This Year*, ZDNET (U.K.) (July 11, 2000, 9:01 AM), http://www.zdnet.co.uk/news/security-management/2000/07/11/hacking-will-cost-world-16-trillion-this-year-2080075/.

[41] *See* Chabinsky, *supra* note 39.

[42] *See* Robert S. Mueller III, Dir., FBI, Address at the RSA Cyber Security Conf., San Francisco, CA: Tackling the Cyber Threat (Mar. 4, 2010) (transcript *available at* http://www.fbi.gov/news/speeches/tackling-the-cyber-threat).

[43] *Compare id.*, *with* Samuel, *supra* note 24[Supra/Infra Error]**Error! Bookmark not defined.**, at 6.

[44] *See* Lawrence Wright, *The Spymaster*, NEW YORKER, Jan. 21, 2008, at 51.

and water purification systems—could have even more catastrophic consequences.[45]

By contrast, hacktivism tends to be motivated by political concerns that are usually at least partly external to the Internet.[46] It is engaged primarily with communicative, not destructive, goals.[47] For example, the defacement of the DOJ web site in protest of the Communications Decency Act of 1996 reflects both political support for individual rights and concerns that the implicated legislation would degrade the culture and value of the Internet through censorship.[48] It also reflects the communicative element of hacktivism, in that the web site remained largely operational during and after the attack, and the cost of repairing the defacement was minimal.[49] Indeed, a significant nexus of hacktivism and hacking is on the issue of censorship, particularly with respect to real or perceived Internet censorship.[50]

C. *Forms of Hacktivism*

For purposes of an analysis of hacktivism as a form of protest, five methods are particularly well-suited for discussion in light of their popularity and the varying degrees to which each resembles legitimate expression.

1. Denial-of-Service Attacks

DoS attacks, the form of hacktivism frequently used during the WikiLeaks incident, involve attempts to deprive service to users of a web site by any of several means.[51] Access to the targeted site can slow significantly or be prevented entirely while the attack is underway.[52]

---

[45] *See* Mark G. Milone, *Hacktivism: Securing the National Infrastructure*, 58 BUS. LAW. 383, 385 (2002).

[46] *See* Samuel, *supra* note 24[Supra/Infra Error]**Error! Bookmark not defined.**, at 14.

[47] *Cf. id.* at 51, 54, 216, 235 (noting that a significant objective of hacktivism is communicating a message).

[48] *Cf. id.* at 9, 42.

[49] *Cf. id.* at 54 (explaining that as a primarily communicative method of hacktivism, web site defacements leave the targeted sites largely unharmed).

[50] *See id.* at 42.

[51] *See* Samuel, *supra* note 24[Supra/Infra Error]**Error! Bookmark not defined.**, at 10; Natasha Lomas, *Security from A to Z: DDoS*, CNET NEWS, (Nov. 27, 2006, 10:57 AM PST), http://news.cnet.com/Security-from-A-to-Z-DDoS/2100-7349_3-6138447.html?tag=mncol;2n.

[52] *See* Samuel, *supra* note 24[Supra/Infra Error]**Error! Bookmark not defined.**, at 10.

During a common type of DoS attack, the party initiating the attack saturates the computer server hosting the target web site with requests for information, dramatically increasing the consumption of computational resources and eventually causing the server to slow down or reset.[53]

A popular iteration of the DoS attack is a distributed denial of service (DDoS) attack, which may be distinguished from a DoS attack by its use of a network of multiple attacking computers.[54] In a DDoS attack, the initiating party activates a network of computers under its control, called a botnet, to multiply the power of the attack, thereby directing an exponentially increased volume of information requests to the target server.[55] So-called because of the manner in which the computers—known as "slaves" or "zombies"—are manipulated by the party initiating the attack, botnets are networks of individual computers that have been infiltrated by a virus or other malicious program that brings them under the control of the infiltrator.[56]

Generally, in order to compromise the security of the infiltrated computer, the virus exploits vulnerabilities in the system.[57] There is no shortage of such vulnerabilities, particularly on home computers and networks.[58] Consequently, botnets are widespread.[59] In fact, reports suggest that the supply of botnets far exceeds demand, leading to a steep drop in their rental price.[60] With so low a barrier to entry, DDoS capability is proliferating.[61]

Unsurprisingly, DDoS attacks have likewise increased substantially in the past few years.[62] Along with enhanced DDoS capacity has come

---

[53] *See Denial of Service Attacks*, CERT Software Eng'g Inst., http://www.cert.org/tech_tips/denial_of_service.html (last visited Apr. 4, 2011).

[54] *See* Charalampos Patrikakis et al., *Distributed Denial of Service Attacks*, Internet Protocol J., Dec. 2004, at 13, *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/ipj_7-4.pdf.

[55] *See id.* at 13, 20; Robert McMillan, *With Botnets Everywhere, DDoS Attacks Get Cheaper*, Computerworld (Oct. 14, 2009, 8:23 PM ET), http://www.computerworld.com/s/article/9139398/With_botnets_everywhere_DDoS_attacks_get_cheaper.

[56] *See* Patrikakis et al., *supra* note 54, at 13; McMillan, *supra* note 55.

[57] *See* Patrikakis et al., *supra* note 54, at 13.

[58] *See* Geer, *supra* note 23, at xi; McMillan, *supra* note 56.

[59] *See* McMillan, *supra* note 56.

[60] *See id.*

[61] *See id.*

[62] *Compare* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 10 (noting that as of 2004, DDoS attacks are rarely used by hacktivists), *with* McMillan, *supra* note 56 (describing an increase in DDoS attacks between 2008–2009).

improved and vastly simplified operating software.[63] The software that was widely used during the WikiLeaks episode was called the Low Orbit Ion Cannon (LOIC), which enabled even novice users to join in the DDoS attacks by making participation relatively simple.[64] LOIC allowed users to participate in the attacks in two ways: directly, by entering the target IP address and essentially clicking "fire;" or, alternatively, by volunteering their system to the so-called "LOIC Hivemind," thereby allowing other users to direct attacks from the surrendered system.[65] The latter option describes a voluntary botnet, in which each computer in the controlled network has effectively been donated for a prescribed use.[66] Unlike members of involuntary botnets, LOIC users retain the ability to remove their computers from the network.[67]

Because of the structure of the Internet, DDoS attacks often implicate the laws of multiple nations.[68] An initiating party located in country A can control a network of computers located in countries B, C, and D to attack a web site hosted on servers located in country E.[69] Thus, the victim, the evidence, and the perpetrator are all located in different countries, many of which likely have different cybersecurity regimes, or no regime at all.[70]

2. Site Defacements

Site defacements, like that perpetrated against the Department of Justice website, are believed to be the most common form of hacktivism.[71] They involve obtaining unauthorized access to a web server and either replacing or altering a web page with new content that conveys a particular message.[72] Defacements may be isolated to a single site, or they may occur in huge volumes across hundreds or thou-

---

[63] *See* George V. Hulme, *LOIC Tool Enables "Easy" WikiLeaks-Driven DDoS Attacks*, CSO Online (Dec. 15, 2010), http://www.csoonline.com/article/646813/loic-tool-enables-easy-wikileaks-driven-ddos-attacks.

[64] *See id.*

[65] *See id.*

[66] *See* Geoff Duncan, *WikiLeaks Supporters Using Volunteer and Zombie Botnets*, Digital Trends (Dec. 9, 2010), http://www.digitaltrends.com/computing/wikileaks-supporters-using-volunteer-and-zombie-botnets/.

[67] *See id.*

[68] *Cf.* Geer, *supra* note 23, at ix.

[69] *Cf. id.*; Patrikakis et al., *supra* note 55, at 20–21.

[70] *See* Ryan M.F. Baron, *A Critique of the International Cybercrime Treaty*, 10 CommLaw Conspectus 263, 270 (2002).

[71] *See* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 9.

[72] *See id.* at 8.

sands of sites.[73] Yet, although they effectively hijack the targeted site in order to communicate a message, defacements do not necessarily damage the targeted site.[74] Instead, site defacements are commonly used not only as a means to communicate a message, but to demonstrate the technical prowess of the defacer; that is, they are as much about seeking attention for the perpetrator as they are about raising awareness for a cause.[75]

3. Site Redirects

As the name suggests, redirects send users to a site that is different than the one indicated by the web address.[76] That is, by gaining unauthorized access to a web server and adjusting the address settings, the perpetrator causes would-be users to reach an alternative site.[77] Quite often, the alternative site is critical of the original, searched-for site.[78] By this method, the hacktivist essentially hijacks access to the targeted site and asserts control over the content that is displayed when an Internet user enters the web address of the targeted site.[79]

4. Virtual Sit-ins

As a form of hacktivism, the virtual sit-in can be compared to a DDoS attack in the sense that the object of both methods is to slow or crash a targeted server by overwhelming it with requests for information.[80] The difference is that rather than commanding a network of voluntary or involuntary botnets, virtual sit-ins involve individual protestors reloading web pages.[81] Some virtual sit-ins have been accomplished simply by users manually and repeatedly reloading the targeted web page; others allowed participants to download special code that automatically and repeatedly reloaded the targeted site.[82]

---

[73] *See id.* at 9.
[74] *See id.* at 54.
[75] *See id.* at 55.
[76] *See id.* at 10.
[77] *See* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 10.
[78] *Id.*
[79] *See id.*
[80] *See id.* at 12.
[81] *See id.*
[82] *See id.* at 12–13.

The virtual sit-in is considered "a mass form of hacktivism . . . [and] a more democratic or representative form of hacktivism."[83]

5. Information Theft

Finally, information theft, a method of hacktivism that is arguably indistinguishable from ordinary burglary, involves gaining unauthorized access to a computer or network and stealing private data.[84] Although the illegality of information theft is probably the least ambiguous of the methods of hacktivism described in this section, it is surprisingly, and distressingly, well-accepted by hacktivists.[85]

II. Discussion

A. *The European Convention on Cybercrime*

Because its drafters deemed international cooperation critical to effective cybercrime regulation, the 2001 Convention on Cybercrime (Convention) prescribes a common criminal policy with regard to cybercrime,[86] and signatory parties are bound to establish domestic criminal laws governing intentional acts of cybercrime.[87] The Convention outlines requirements for substantive laws concerning offences against the integrity of computer data and systems.[88]

1. Definitions

Article 2 of the Convention requires regulation of illegal access to computer systems.[89] Parties are obligated to enact criminal laws prohibiting access to any part of a computer system "without right."[90] Article 2 specifies that such access may be obtained either by circum-

---

[83] Samuel, *supra* note 24**Error! Bookmark not defined.**, at 12.

[84] *Id.* at 11.

[85] *See id.* at 123, 137, 143–44.

[86] *See* Convention on Cybercrime pmbl., Nov. 23, 2001, 2296 U.N.T.S. 167 [hereinafter Convention].

[87] *See id.* at art. 2. The Convention mandates that Signatories create new cybercrimes, which may not have been recognized as offenses under existing legal regimes. *See* Baron, *supra* note 70, at 270.

[88] *See id.* at sec. 1.

[89] *See id.* at art. 2. The Convention defines computer systems as devices, either free-standing or networked with other devices, that perform automatic data processing using a program. *Id.* at art. 1(a).

[90] *Id.* at art. 2.

venting security measures or by exploiting authorized access to one system to gain unauthorized access to other systems.[91] In addition, the Article states that Parties may require that unlawful access be motivated by intent to obtain computer data or other dishonest intent.[92]

The Convention also requires Parties to establish criminal laws prohibiting the intentional, unauthorized interception of computer data. [93] Article 3 specifies that such interception should be prohibited when it is accomplished by technical means and when the intercepted data is part of a non-public transmission.[94] Moreover, the Article prohibits interception of "electromagnetic emissions" from computer systems.[95]

Similarly, Articles 4 and 5 respectively require Parties to prohibit interference with both data and systems.[96] The Convention provides that data interference may be accomplished when a person intentionally and without authorization damages, deletes, deteriorates, alters, or suppresses computer data.[97] Further, Article 4 states that Parties are permitted to require that data interference result in serious harm before criminal liability attaches.[98] Article 5 obligates Parties to prohibit intentional system interference.[99] Actions cause system interference when they seriously hinder the functioning of a computer system by the inputting or transmitting of data, or the manipulation of data by many of the same means involved in data interference.[100]

In addition to outlining a regime of criminal laws governing data and computer systems, the Convention also describes laws regarding the misuse of devices.[101] Unlike the provisions governing data and computer systems, Article 6 does *not* to impose liability so long as the devices in question are not used to commit offenses set forth in Articles 2 through 5.[102] For devices that are designed or adapted primarily to intercept or interfere with data or systems, however, Parties are ob-

---

[91] *See id.*

[92] *See* Convention, *supra* note 86, at art. 2.

[93] *Id.* at art. 3. Computer data is defined as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function." *Id.* at art. 1(b).

[94] *Id.* at art. 3.

[95] *Id.*

[96] *See id.* at arts. 4, 5.

[97] Convention, *supra* note 86, at art. 4(1).

[98] *Id.* at art. 4(2).

[99] *Id.* at art. 5.

[100] *See id.* at art. 5.

[101] *See id.* at art. 6.

[102] *See id.* at art. 6(2).

ligated to enact laws prohibiting their possession, "production, sale, procurement for use, import, distribution or otherwise" being made available if they are intended for use in the commission of offenses under Articles 2 through 5.[103] Furthermore, Article 6 imposes the same restrictions on computer passwords, access codes and similar information capable of accessing any part of a computer system.[104]

2. The Domestic Regimes

The Convention outlines requirements for domestic laws regarding computer-related offenses.[105] Article 7 mandates that Parties establish anti-forgery laws to prohibit the intentional, unauthorized manipulation or fabrication of data that results in inauthentic data intended to be accepted as genuine.[106] The Article further stipulates that Parties are free to condition criminal liability on intent to defraud or other dishonest intent.[107] Relatedly, Article 8 describes anti-fraud laws to prohibit interference with or manipulation of data or systems by which victims are deprived of property with the fraudulent intent of procuring an economic benefit for the perpetrator.[108]

Finally, the Convention requires parties to establish laws concerning "offences related to infringements of copyright and related rights,"[109] and to establish a legal regime governing ancillary and corporate liability for accessories to cybercrime.[110] The Convention is not exhaustive of the possible forms of cybercrime, however, and it authorizes Parties to enact laws regarding all "other criminal offences committed by means of a computer system."[111]

3. Enforcement Provisions

The Convention requires Parties to establish procedures to allow domestic law enforcement to implement the new laws and investigate and prosecute cybercrimes.[112] It also stipulates that Parties cooperate

---

[103] Convention, *supra* note 86, at art. 6(1).
[104] *Id.*
[105] *See id.* at tit. 2.
[106] *Id.* at art. 7.
[107] *Id.*
[108] *Id.* at art. 8.
[109] Convention, *supra* note 86, at art. 10.
[110] *See id.* at tit. 5.
[111] *See id.* at art. 14(2).
[112] *See id.* at art. 14(1).

with each other in the enforcement of cybercrime laws.[113] The Convention describes extradition arrangements that, although conditioned by any pre-existing extradition treaty between Parties, provide for the extradition of suspects from one Party state to another to face charges arising from cybercrime laws enacted under the Convention.[114] In addition, the Convention provides for mutual assistance between Parties for purposes of investigating and prosecuting cybercrimes.[115]

Beyond mandating the establishment of domestic cybercrime laws, though, the Convention requires that the implementation and application of laws enacted under the Convention accord with international agreements concerning the protection of human and civil rights.[116] Specifically, Article 15 refers to the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and "other applicable international human rights instruments."[117] The Article requires incorporation of the principle of proportionality, and provides that judicial supervision should be provided where appropriate.[118] Lastly, Article 15 obligates Parties to consider the impact of such laws on the rights and interests of third parties.[119]

B. *The American System*

1. The Computer Fraud and Abuse Act of 2006

At least forty different federal statutes govern computer-related crimes in the United States.[120] Foremost among these for the regulation of hacking and, potentially, hacktivism, is the Computer Fraud and Abuse Act of 2006 (CFAA).[121] Under the statute, seven categories of conduct are prohibited as they relate to "protected computers," which are defined as:

---

[113] *Id.* at art. 23.
[114] *Id.* at art. 24.
[115] Convention, *supra* note 86, at art. 25, 27–34.
[116] *Id.* at art. 15.
[117] *Id.*
[118] *Id.* at art. 15.
[119] *Id.* at art. 15(3).
[120] *See* McCurdy, *supra* note 23, at 300.
[121] 18 U.S.C. § 1030 (2006); *see* McCurdy, *supra* note 23, at 304.

> [A] computer . . . used by or for a financial institution or the United States Government . . . or, which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[122]

In other words, any computer in the United States that is connected to the Internet, and even some foreign computers, are subject to the CFAA.[123] Subsection (a)(1) of the statute prohibits obtaining or transmitting classified information as a result of unauthorized computer access if the actor has "reason to believe" the information could be used either to the detriment of the United States, or to the advantage of any foreign nation.[124] The next subsection prohibits obtaining financial information, information from any government entity, or information from any "protected computer," through unauthorized computer access.[125] Third, the CFAA forbids unauthorized access of any nonpublic computer of the United States government.[126] Subsection (a)(4) proscribes unauthorized computer access with intent to defraud and obtain something of value.[127]

The fifth subsection, § 1030(a)(5), is directed specifically at hacking.[128] The provision describes two distinct types of offenses.[129] The first type involves knowingly transmitting "a program, code or command that intentionally causes damage to a protected computer," regardless of whether the actor had authorized access.[130] The second type of offense involves unauthorized access of a protected computer that causes damage.[131] This type of offense does not require intent to cause damage or loss, and liability can attach as a result of either recklessness or negligence.[132]

The sixth subsection forbids the knowing trafficking of passwords or similar information with intent to defraud that permits unauthorized computer access if the trafficking affects interstate or foreign

---

[122] *Id.* § 1030(e)(2); *see* McCurdy, *supra* note 23, at 304–05.
[123] McCurdy, *supra* note 23, at 304; *see* § 1030(e)(2).
[124] § 1030(a)(1).
[125] § 1030(a)(2).
[126] § 1030(a)(3).
[127] § 1030(a)(4).
[128] *See* § 1030(a)(5); McCurdy, *supra* note 23, at 305.
[129] *See* § 1030(a)(5)(A); McCurdy, *supra* note 23, at 305.
[130] McCurdy, *supra* note 23, at 305; *see* § 1030(a)(5)(A)(i).
[131] *See* § 1030(a)(5)(A)(ii)–(iii); McCurdy, *supra* note 23, at 305.
[132] *See* § 1030(a)(5)(A)(iii); McCurdy, *supra* note 23, at 305.

commerce, or if the accessed computer is used by or for the United States government.[133] Finally, subsection § 1030(a)(7) prohibits the transmission with intent to extort in interstate or foreign commerce of any communication which threatens damage to a protected computer; threatens to obtain unauthorized access to a protected computer and retrieve or impair the confidentiality of information stored thereon; or extorts money in relation to damage to a protected computer.[134]

2. A Primer on the Jurisprudence of Protest

The distinction between permissible protest and impermissible disruption has been a subject of controversy for generations.[135] According to the U.S. Supreme Court, "the right to engage in peaceful and orderly political demonstrations is, under appropriate conditions, a fundamental aspect of 'liberty' protected by the Fourteenth Amendment."[136] What is more, even protests that rile the audience or cause excitement that is potentially disruptive to the civic peace are generally protected so long as they are not "directed to inciting or producing imminent lawless action and [are] likely to incite or produce such action."[137] In the context of the First Amendment, contributions to the public debate on matters of public concern are considered essential to a functioning democracy,[138] and the Supreme Court has been extremely reluctant to allow punishment of false or even grievously offensive speech in this area.[139]

---

[133] § 1030(a)(6)

[134] § 1030(a)(7).

[135] *See, e.g.*, City of Chicago v. Morales, 527 U.S. 41, 56–60 (1999) (striking down city anti-loitering statute as unconstitutionally vague and violative of due process under the Fourteenth Amendment); Street v. New York, 394 U.S. 576 *passim* (1969) (overturning criminal conviction arising from public desecration of American flag and associated comments made to assembled crowd); Smith v. Donnelly, (2001) S.L.T. 1007, 1012 (Scot.) (appealing conviction for breach of peace on grounds that protest caused severe disturbance in community).

[136] Shuttlesworth v. City of Birmingham, 394 U.S. 147, 161 (1969) (Harlan, J., concurring).

[137] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

[138] *See* Cantwell v. Connecticut, 310 U.S. 296, 310 (1940). In an important and oft-quoted passage, Justice Roberts declared that "the people of this nation have ordained in the light of history, that, in spite of the probability of excesses and abuses, these liberties are, in the long view, essential to enlightened opinion and right conduct on the part of the citizens of a democracy." *Id.*

[139] *See id. See also* Snyder v. Phelps, 131 S. Ct. 1207, 1220 (2011) (declaring that "[a]s a Nation we have chosen a different course—to protect even hurtful speech on public issues

The government's ability to limit protest by imposing reasonable time, place and manner restrictions on speech, however, is largely unquestioned.[140] In this sense, protests can be *channeled*, but not stifled completely, even if they are peaceful and involve matters of public concern.[141] Restrictions of this kind must be "content-neutral," in that they cannot prohibit speech on the basis of its subject matter or the speaker's identity or viewpoint, they must serve a significant government interest, and they must leave open ample alternative avenues for communication.[142] Moreover, the Court has recognized that such restrictions are permissible even on speech that occurs in areas, like public streets, that traditionally have been used for the exchange of ideas.[143] In the context of the Internet, and as applied specifically to hacktivism, it is not entirely clear what form a permissible time, place and manner restriction can take.[144]

In addition, the public forum doctrine generally protects speech in "places which by long tradition or by government fiat have been devoted to assembly and debate."[145] In a public forum, the government may impose content-neutral time, place and manner restrictions.[146] It may also impose a licensing or permit system for the

---

to ensure that we do not stifle public debate") *available at* http://www.supremecourt.gov/opinions/10pdf/09-751.pdf; N.Y. Times Co. v. Sullivan, 376 U.S. 254 *passim* (1964) (overturning jury verdict of defamation against newspaper for allegedly harmful statements in full-page issue advertisement concerning treatment of civil rights protestors by police and state officials).

[140] *See, e.g.*, Frisby v. Shultz, 487 U.S. 474, 487 (1988) (upholding municipal ordinance prohibiting residential picketing directed at and occurring in front of a residence); Police Dept. of Chicago v. Mosley, 408 U.S. 92, 98–99 (1972) (invalidating municipal anti-picketing ordinance on equal protection grounds but recognizing government's ability to regulate picketing and other forms of protest through reasonable time, place, and manner restrictions); Kovacs v. Cooper, 336 U.S. 77, 83 (1949) (upholding municipal ordinance prohibiting use of sound trucks on public streets).

[141] *See, e.g.*, *Frisby*, 487 U.S. at 487; *Mosley*, 408 U.S. at 98–99; *Kovacs*, 336 U.S. at 83.

[142] *See* City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 47 (1986).

[143] *See Kovacs*, 336 U.S. at 87. Writing for a plurality, Justice Reed noted that "[c]ity streets are recognized as a normal place for the exchange of ideas by speech or paper. But this does not mean the freedom is beyond all control." *Id.*

[144] The Supreme Court has yet to address the question of time, place and manner restrictions of Internet conduct, and the decisions of lower courts have been limited primarily to a variant of the question involving registration of domain names. *See e.g.*, Name. Space, Inc. v. Network Solutions, Inc., 202 F.3d 573, 587 (2d Cir. 2000) (finding that an amendment to an agreement of U.S. Department of Commerce concerning competition in domain name registration was a valid time, place and manner restriction).

[145] Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

[146] *See, e.g.*, Hill v. Colorado, 530 U.S. 703, 714 (2000) (upholding state law limiting protest outside health care facilities); Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 289 (1984) (upholding National Park Service regulation prohibiting sleeping over-

use of public forums so long as it serves an important purpose, leaves virtually no discretion to the licensing authority, and provides procedural safeguards including judicial review of license denials.[147] The doctrine also has potential ramifications for speech on private property as well, if the property is open to the public.[148] It is as yet unclear how, if at all, the Supreme Court will apply the public forum in the context of the Internet.[149]

C. *The British System*

1. The Computer Misuse Act of 1990

In the United Kingdom, acts of hacktivism generally fall under the Computer Misuse Act of 1990 (CMA).[150] Unlike the American CFAA, the CMA does not define the machines protected by its provisions.[151] Instead, the statute prohibits unauthorized access to "computer material" and defines the actions to which criminal liability will attach.[152] Section 1 provides that a person violates the CMA by knowingly and intentionally gaining unauthorized access to programs or data held in any computer.[153] The provision clarifies the intent requirement by noting that the perpetrator need not intend to gain access to a particular program or data of any kind on any computer; intentionally gaining unauthorized access to the information is sufficient for culpability.[154] The section further states that the maximum sentence of incarceration is two years.[155]

---

night in public parks); Cox v. New Hampshire, 312 U.S. 569, 576 (1941) (affirming convictions for violations of municipal ordinance requiring special permit for parades).

[147] *See Cox*, 312 U.S. at 576.

[148] *See* PruneYard Shopping Ctr. v. Robins, 447 U.S. 74, 79 (1980) (affirming state supreme court decision upholding state constitutional amendment protecting speech in privately-owned shopping centers, and thereby preventing property owners from excluding certain speakers).

[149] *See* United States v. Am. Library Ass'n, Inc., 539 U.S. 194, 215 (2003) (Breyer, J., concurring) (noting that the public forum doctrine is inapplicable as applied to a statute conditioning receipt of federal funds on implementation of filtering software in public libraries).

[150] Computer Misuse Act, 1990, c. 18 (U.K.) (amended 2008), *available at* http://www.legislation.gov.uk/ukpga/1990/18/data.pdf.

[151] *Id.* § 1.

[152] *Id.*

[153] *Id.* § 1(1).

[154] *Id.* § 1(2).

[155] *Id.* § 1(3).

Section 2 of the CMA prohibits actions that violate Section 1 and that are taken with intent to commit further offenses, or to allow others to commit offenses by means of unauthorized access.[156] Specifically, Section 2 applies to offenses for which there are statutorily fixed sentences or to offenses carrying sentences of five years or more.[157] The further offenses need not occur at the same time as unauthorized access is gained, nor even be possible; that is, the section prohibits arranging for further offenses even if such offenses are in fact impossible.[158] The maximum sentence for offenses under this section is five years.[159]

Particularly relevant to DDoS attacks and site defacements, Section 3 prohibits unauthorized acts that impair the operation of a computer, prevent or hinder access to programs or data on a computer, or enable others to impair computer operations or hinder access to systems.[160] A person violates Section 3 if he knowingly does "any unauthorised act in relation to a computer."[161] Notably, liability attaches under this section even if the acts are not intentional, but simply reckless.[162]

As with Section 2, a prohibited act need not be intended to affect a particular computer, program or data; the act need only be intended to have some effect on some computer, program or data.[163] The Section further specifies that acts whose effect is only temporary are nevertheless prohibited, as if the effect was permanent.[164] The maximum sentence under this section is ten years.[165]

Section 3A prohibits making, supplying, or obtaining "articles" to be used in offenses under Sections 1 and 3.[166] "Article" is defined as any program or data held in electronic form.[167] This provision is violated if a person supplies or offers to supply an item believing that it is likely to be used to commit or assist in the commission of an act which

---

[156] Computer Misuse Act, § 2(1).
[157] *Id.* § 2(2).
[158] *Id.* § 2(3)–(4).
[159] *Id.* § 2(5).
[160] *Id.* § 3(2).
[161] *Id.* § 3(1).
[162] Computer Misuse Act, § 3(4).
[163] *See id.* § 3(4).
[164] *See id.* § 3(5)(c).
[165] *Id.* § 3(6).
[166] *Id.* § 3A.
[167] *Id.* § 3A(4).

violates Sections 1 or 3.[168] Violations under Section 3A are punishable by a maximum sentence of two years.[169]

Section 4 of the CMA describes the territorial scope of offenses under Sections 1 through 3. Although it requires "at least one significant link with domestic jurisdiction,"[170] the section states that it is "immaterial" whether the offense itself was committed in the United Kingdom, or whether the accused was in the United Kingdom when the offense was committed.[171] The "significant links with domestic jurisdiction" are addressed in Section 5, which provides that either the accused person's presence in the United Kingdom at the time the act was committed, or the presence of the computer that was wrongfully accessed, constitute a significant link with domestic jurisdiction.[172]

2. British Courts and the Right of Expression

In the United Kingdom, free speech receives less robust protection than in the United States.[173] Indeed, some argue that free speech in the United Kingdom is almost totally reliant on "cultural norms to check the abuse of government power to restrict or ban expression."[174] Judicial review with respect to laws restricting speech is largely non-existent; the freedom of speech is protected nearly exclusively by Parliamentary "self-control."[175] The United Kingdom does not have a written constitution, and the only textual protection for speech rights is the Human Rights Act of 1998,[176] which codifies, among oth-

---

[168] Computer Misuse Act, § 3A(2).

[169] *Id.* § 3A(5).

[170] *Id.* § 4(2).

[171] *Id.* § 4(1).

[172] *Id.* § 5(2)–(3).

[173] *See, e.g.*, Ronald J. Krotoszynski, Jr., The First Amendment in Cross-Cultural Perspective: A Comparative Legal Analysis of the Freedom of Speech 184–85 (2006) (describing the speech restrictions permissible in the United Kingdom under the Human Rights Act 1998); Michael L. Rustad & Thomas H. Koenig, *Harmonizing Internet Law: Lessons from Europe*, J. Internet L., May 2006, at 3 (noting stronger protections for speech in the United States than in the United Kingdom); Francis Welch, *The "Broadcast Ban" on Sinn Fein*, BBC News (Apr. 5, 2005), http://news.bbc.co.uk/2/hi/uk_news/politics/4409447.stm (describing British government's direct broadcast ban for organizations in Northern Ireland thought to support terrorism).

[174] Krotoszynski, *supra* note 173, at 187.

[175] *Id.* at 187–88.

[176] *Id.* at 184.

er things, Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[177]

This is not to say that speech rights are unprotected in the United Kingdom; to the contrary, at common law free speech is a legal principle to be considered by courts interpreting acts of Parliament or deciding cases that implicate speech rights.[178] British courts frequently have invoked the common law principle to cabin laws that would otherwise inhibit the exercise of free speech.[179] In libel cases, for example, British courts have formulated fair comment and privilege defenses that protect speech.[180] Principles of free speech derived from the common law have also been invoked to limit the scope of legislation that could have restricted speech rights.[181]

Nevertheless, partly because of the absence of a constitutional guarantee of free speech, common law presumptions require a balancing of speech rights against other, competing, rights that may weigh against free speech.[182] In addition, there has been little consideration in British courts of the extent of free speech rights outside certain, well-established areas of law—namely, defamation, breach of confidence, and contempt of court.[183] As a result, the principle of free speech in the United Kingdom remains limited at common law.

III. Analysis

A. *Hacktivism as Legitimate Protest*

As an initial matter, to carve out protection for hacktivism in the existing anti-hacking legal regime, a distinction is necessary between harmful, and thus rightly prohibited, forms of hacking, and types of

---

[177] *See id.* at 183. Article 10 of the Human Rights Convention provides that "[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." Convention for the Protection of Human Rights and Fundamental Freedoms art. 10(1), Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR]. The freedoms described in paragraph 1 are qualified, however, by paragraph 2, which declares that "[t]he exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such . . . restrictions or penalties as are prescribed by law and are necessary in a democratic society." *Id.* at art. 10(2).

[178] *See* Eric Barendt, Freedom of Speech 41 (2d ed. 2005).

[179] *See id.* at 40.

[180] *See id.*

[181] *See id.* at 41.

[182] *See id.* at 41–42.

[183] *See id.* at 42.

hacktivism that sufficiently resemble traditional protest so as to warrant protection.[184] Unsurprisingly, this is much easier said than done.[185]

Just as traditional means of protest can cause inconvenience and frustration among both the object of the protest and the general public, hacktivism, too, can look more like a nuisance than an exercise of protected rights of expression and dissent.[186] And the unique forum of online protest—i.e., cyberspace, which exists on privately-owned servers, and yet functions as a global public square[187]—further complicates the question whether the Internet is an appropriate situs for demonstration.[188] Nevertheless, the same democratic interests that require toleration of the burdens on the normal functioning of society imposed by civil demonstration in the physical world demand that a narrow subset of hacktivism be protected as legitimate forms of political protest.[189] Given that hacktivism may take a wide variety of forms,[190] to separate the "good" hacktivism from the "bad," it is useful first to establish some parameters. This Note argues that those forms of hacktivism that are primarily expressive, that do not involve obtaining or exploiting illegal access to computers or networks for commercial advantage or financial gain, and that cause little or no permanent damage should receive at least some protection as a legitimate form of protest.

1. Hacktivism as Protected Expression

To warrant protection, it is not sufficient that hacktivism merely convey a message; the world over, graffiti bans are accepted as reasonable and necessary measures to deter damage to both public and pri-

---

[184] *See, e.g.*, *WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, Economist, Dec. 16, 2010, *available at* http://www.economist.com/node/17732839 [hereinafter Economist].

[185] *See id.*; Terrence O'Brien, *Protesting Hacktivists Replacing Picket Lines With Web Attacks*, Switched (Feb. 11, 2010, 7:35 AM), http://www.switched.com/2010/02/11/protesting-hacktivists-replacing-picket-lines-with-web-attacks/.

[186] *See* Economist, *supra* note 184.

[187] *Cf.* James Grimmelmann, *The Internet is a Semicommons*, 78 Fordham L. Rev. 2799, 2799–800 (2009) (describing Internet's combination of private network infrastructure with "a commons in the communications that flow through the network").

[188] *See* Jeremy A. Kaplan, *We Want YOU, Say Hacktivists . . . But Is It Legal?*, Fox News (Dec. 9, 2010), http://www.foxnews.com/scitech/2010/12/09/wikileaks-operation-payback-hacktivists-legal/.

[189] *See* Economist, *supra* note 184.

[190] *See* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 7.

vate property.[191] Even in the United States, where speech rights are jealously guarded by the First Amendment, not all expression receives protection.[192] Hacktivism that causes damage—e.g., information theft—or involves the manipulation of hijacked private property—e.g., DDoS attacks using involuntary botnets—is not likely to be considered expression at all.[193]

Like protestors in a picket line, hacktivism within the jurisdiction of the United States should be subject to reasonable restrictions on the time, place and manner of the demonstration.[194] While it is not at all clear what such restrictions would look like in the context of the Internet, given the often critical importance of certain web sites as a source of vital information, restrictions on otherwise permissible cyberprotests are likely in many circumstances.[195] For example, virtual

---

[191] *See, e.g.*, Ian Edwards, *Banksy's Graffiti: A Not-So-Simple Case of Criminal Damage?*, 73 J. Crim. L. 345, 345 (2009) (discussing possible prosecution of graffiti artists under the U.K.'s Criminal Damage Act of 1971).

[192] *See, e.g.*, Miller v. California, 413 U.S. 15, 24 (1973) (upholding conviction for violation of state obscenity law on grounds that, *inter alia*, the material lacked "serious literary, artistic, political, or scientific value").

[193] *See, e.g.*, Charlie Savage, *Soldier Faces 22 New WikiLeaks Charges*, N.Y. Times, Mar. 2, 2011, at A6, *available at* https://www.nytimes.com/2011/03/03/us/03manning.html (describing charges against U.S. soldier accused of facilitating WikiLeaks' disclosure of classified government documents); Michael Cooney, *FBI: Operation Bot Roast Finds Over 1 Million Botnet Victims*, Network World (June 13, 2007), http://www.networkworld.com/community/node/16193 (describing FBI investigation and arrest of controllers of involuntary botnets).

[194] *See, e.g.*, Frisby v. Shultz, 487 U.S. 474, 487 (1988) (upholding municipal ordinance prohibiting residential picketing directed at and occurring in front of a residence); Police Dept. of Chicago v. Mosley, 408 U.S. 92, 98–99 (1972) (invalidating municipal anti-picketing ordinance on equal protection grounds but recognizing government's ability to regulate picketing and other forms of protest through reasonable time, place, and manner restrictions); Kovacs v. Cooper, 336 U.S. 77, 87 (1949) (upholding municipal ordinance prohibiting use of sound trucks on public streets).

[195] The Supreme Court has not yet addressed time, place, and manner restrictions in the context of the Internet; however, because hacktivism can take forms that are analogous to traditional methods of protest, restrictions on those forms should be no greater than those imposed on the traditional methods. *Compare* City of Ladue v. Gilleo, 512 U.S. 43, 48 (1994) (invalidating municipal ordinance prohibiting display of yard signs on private property), Martin v. City of Struthers, 319 U.S. 141, 146–47 (1943) (invalidating municipal ordinance against door-to-door distribution of handbills), *and* Schneider v. State, 308 U.S. 147, 162 (1939) (invalidating municipal anti-leafleting ordinance), *with* Heffron v. Int'l Soc'y for Krishna Consciousness, 452 U.S. 640, 651 (1981) (upholding state regulation prohibiting sale or distribution of merchandise and literature except from a booth rented from the state, on grounds that state had sufficiently substantial interest in regulating solicitation activities at fairgrounds), Greer v. Spock, 424 U.S. 828, 838 (1976) (upholding exclusion of political candidates from military base on grounds that "the business of a military installation . . . is to train soldiers, not to provide a public forum), *and* Adderley v. Florida, 385 U.S. 39, 47–48 (1966) (upholding convictions of civil rights protestors for

sit-ins waged against the official web site of an incumbent political officeholder that might conceivably be otherwise protected could be prohibited in the period leading up to an election.[196] Or, while a virtual sit-in on the web site of a high school might be permissible—in response, perhaps, to a decision by the administration to cancel prom—the same attack made by students on the web site of a high school newspaper that published an editorial supporting the decision could be punished on the theory that the state has a substantial interest in controlling the terms of debate in secondary schools.[197] Assuming *arguendo*—as one must, given the embryonic state of the law—that the use of these methods would be cognizable as protected expression, they likely would be subject to all manner of other restrictions that the Supreme Court has recognized as consistent with the First Amendment.[198]

---

trespass at jail on grounds that "[t]he State, no less than a private owner of property, has power to preserve the property under its control for the use to which it is lawfully dedicated").

[196] *Cf.* City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789, 807–08 (1984) (upholding municipal regulation prohibiting posting signs on public property as applied to individuals who attached political advertisements to utility poles); *Political Hacktivists Turn to Web Attacks*, BBC News (Feb. 10, 2010), http://news.bbc.co.uk/2/hi/technology/8506698.stm (describing Australian "cyber-activists" blocking government websites to protest proposals to filter content). *But cf.* Citizens United v. Fed. Election Comm'n, 130 S. Ct. 876, 1 (2010) (striking down on First Amendment grounds limits on campaign expenditures by corporations), *available at* http://www.supremecourt.gov/opinions/09pdf/08-205.pdf.

[197] *Cf.* Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260, 270–71 (1988) (upholding high school principal's exclusion of two stories from student newspaper on grounds that educators properly retain near-total control over school activities that might reasonably be perceived "to bear the imprimatur of the school"); Bethel Sch. Dist. v. Fraser, 478 U.S. 675, 683 (1986) (upholding punishment of high school student for vulgar speech given in context of student election); Tinker v. Des Moines Sch. Dist., 393 U.S. 503, 509 (1969) (holding that student expression cannot be suppressed unless it will materially or substantially disrupt the work and discipline of the school). *But cf.* Papish v. Bd. of Curators, 410 U.S. 667, 671 (1973) (finding that state university violated First Amendment when it expelled a graduate student for distributing newspaper on campus featuring political cartoon depicting a policeman raping the Statue of Liberty and the Goddess of Justice).

[198] *See, e.g.*, *Cox*, 312 U.S. at 576 (affirming convictions for violations of municipal ordinance requiring special permit for parades); *Kovacs*, 336 U.S. at 87 (upholding municipal ordinance prohibiting use of sound trucks on public streets); *Miller*, 413 U.S. at 36–37 (upholding conviction for violation of state obscenity law on grounds that, *inter alia*, the material lacked "serious literary, artistic, political, or scientific value."); *Cmty. for Creative Non-Violence*, 468 U.S. at 289 (upholding National Park Service regulation prohibiting sleeping overnight in public parks); *Frisby*, 487 U.S. at 487 (upholding municipal ordinance prohibiting residential picketing directed at and occurring in front of a residence); *Hill*, 530 U.S. at 714 (upholding state law limiting protest outside health care facilities).

Hacktivism in the United Kingdom is likely to be even more tightly restricted and less likely to be considered protected expression, notwithstanding the passage of the Human Rights Act of 1998 (HRA).[199] In the context of the WikiLeaks controversy, this premise will almost certainly be tested in the near future as members of Anonymous have "declared war" on the British government.[200] Indeed, reports indicate that at least five people have already been arrested in the United Kingdom under the CMA for their role in attacks related to the WikiLeaks controversy.[201] Given the wide discretion accorded to British courts in the application of common law principles in statutory interpretation, and in light of the uncertainty surrounding the interpretation of the HRA,[202] as such attacks proliferate it is likely that acts of hacktivism of all varieties will be prosecuted.[203]

It will not be surprising if British courts refuse to recognize a free speech exception to the CMA, even under the HRA, for hacktivism.[204] There is some precedent, however, that might support finding that punishment of certain forms of hacktivism would infringe speech rights.[205] But recent trends suggest that at least in the near future, the

---

[199] *See* Barendt, *supra* note 178, at 43 (noting that while the HRA incorporates the guarantee of the right of free expression in Article 10 of the ECHR, "[i]t is unclear what functions are covered by this clause"); Krotoszynski, *supra* note 159, at 190 (noting that while "British courts do not possess a direct constitutional command to consider free speech claims[,] . . . [t]he HRA now establishes a statutory right to the freedom of speech").

[200] Jerome Taylor, *WikiLeaks "Hacktivists" Declare War on the UK*, Independent (Feb. 1, 2011), http://www.independent.co.uk/news/media/online/wikileaks-hacktivists-declare-war-on-the-uk-2200172.html.

[201] *Id.*

[202] *See* Barendt, *supra* note 178, at 41–42 (discussing that common law presumptions require a balancing of speech rights against other rights that may weigh against free speech).

[203] *See* Taylor, *supra* note 200 (noting criticism of British government's cybersecurity preparedness and vulnerability to DDoS attacks in light of threat of mass cyber protests).

[204] *Compare* R v. Shayler, [2002] UKHL 11, [2003] 1 A.C. 247 (H.L.) [6], [36] (appeal taken from Eng.) (finding that disclosure of information by former member of security service "in the public and national interest" by Official Secrets Act of 1989 was not protected by freedom of expression under HRA), *with* Krotoszynski, *supra* note 159, at 206 (describing a "rare burst of judicial activism" in which the Law Lords "took upon themselves the task of safeguarding the . . . right to free expression").

[205] *See, e.g.*, Brutus v. Cozens, [1973] A.C. 854 (H.L.) 863 (appeal taken from Eng.) (affirming dismissal of charges of using insulting behavior whereby a breach of the peace was likely to be occasioned on ground that means of protest in question were not insulting); R v. Home Secretary, ex p Simms [2000] 2 A.C. 115 (H.L.) 130–31 (finding that provisions of Prison Service Standing Orders should not be construed to ban prisoners from giving interviews to journalists on grounds that doing so would infringe prisoners' speech rights). Lord Reid, the renowned common law judge, found that "Parliament had to solve the

British government may be more inclined to suppress protest, particularly if such a ban did not pose a risk of provoking greater opposition.[206] In the case of the Anonymous DDoS attacks, government crackdowns have already begun.[207] Whether or not the courts or Parliament will recognize these attacks as a protectable form of expression is yet to be seen.[208]

To the extent that an act of hacktivism is expressive, however, it should be eligible for protection as a form of legitimate protest.[209] Certain forms of hacktivism—namely, virtual sit-ins and voluntary DDoS attacks—closely resemble traditionally accepted forms of protest, like physical sit-ins and picket lines.[210] This is not to say that an act of hacktivism's expressive nature, standing alone, should be sufficient to guarantee immunity; but, like forms of peaceful demonstration that have historically received presumptive First Amendment pro-

---

difficult question of how far freedom of speech or behaviour must be limited in the general public interest. It would have been going much too far to prohibit all speech or conduct likely to occasion a breach of the peace. . ." and, therefore, "vigorous and it may be distasteful or unmannerly speech . . . is permitted so long as it does not go beyond any one of three limits. It must not be threatening. It must not be abusive. It must not be insulting." *Brutus*, [1973] A.C. 854 at 862.

[206] *See, e.g.*, Mark Hughes, *Student Protests May Be Banned Altogether if Violence Continues*, Independent (Dec. 15, 2010), http://www.independent.co.uk/news/uk/crime/student-protests-may-be-banned-altogether-if-violence-continues-2160620.html (describing Scotland Yard's proposal to request a ban on street marches if violence associated with ongoing protests does not subside).

[207] *See* Steve Ragan, *Five Arrested in U.K. Raid on Anonymous*, Tech Herald (Jan. 27, 2011), http://www.thetechherald.com/article.php/201104/6749/Five-arrested-in-U-K-raid-on-Anonymous (describing raids by the Metropolitan Police Service's Police Central e-Crime Unit to arrest members of Anonymous for participating in DDoS attacks as part of Operation: Payback).

[208] *See id.* (describing the discretion given to police to prohibit street demonstrations); *supra* text accompanying notes 173–83 (describing limited textual protection for free expression and discretion granted to courts and Parliament to restrict speech in favor of other interests).

[209] *Cf.* Texas v. Johnson, 491 U.S. 397, 399 (1989) (overturning conviction for violation of state flag desecration statute on First Amendment grounds).

[210] *See* Taylor, *supra* note 200 (quoting Anonymous' belief that the "right to peacefully protest is one of the fundamental pillars of any democracy and should not be restricted in any way"). *Compare* Duncan, *supra* note 66 (describing popular use of LOIC and Hivemind software as part of voluntary DDoS attacks), *with* James Dickson, *Ann Arbor Man Part of Sit-In at Sen. John McCain's Tuscon Office*, Ann Arbor.com (May 17, 2010, 5:46 PM), http://www.annarbor.com/news/ann-arbor-man-partakes-in-immigration-rights-sit-in-at-sen-john-mccains-tuscon-office/ (describing sit-in at U.S. Senator's office in protest of Senator's immigration policies and noting Senator's acknowledgment of the protestors' "right to peacefully protest").

tection, so too should acts of hacktivism that are primarily expressive.[211]

2. Hacktivism, not Hijacking

Although the United States Supreme Court has recognized that some private property owners are limited in their ability to exclude speakers from their property, it is far from clear whether it would tolerate the kind of hijacking of property that occurs through the use of some forms of hacktivism.[212] Website defacements, for example, are unlikely to be protected in part because they involve hacking into web servers and replacing the owners' content.[213] Moreover, lower courts have interpreted the CFAA to prohibit the hijacking of third party computers, by a bot or by other means, in order to access a website; thus, even voluntary DDoS attacks could be considered violations of the statute.[214] And it should go without saying that acts like information theft will almost invariably be condemned under any statute.[215] The same is true of acts that are undertaken with a view to obtaining commercial or financial advantage.[216]

---

[211] *See* Cox v. Louisiana, 379 U.S. 536, 546, 547 (1965) (overturning conviction for breach of the peace on the grounds that no conduct occurred "which the State had a right to prohibit as a breach of the peace"); Edwards v. South Carolina, 372 U.S. 229, 235 (1963) (finding that arrest and conviction of peaceful protestors on charge of breaching the peace "infringed the [protestors'] constitutionally protected rights of free speech, free assembly, and freedom to petition for redress of their grievances"); Cantwell v. Connecticut, 310 U.S. 296, 310 (1940) (articulating the principle that the First Amendment requires that unpleasant and even insulting speech be tolerated).

[212] *Cf.* PruneYard Shopping Ctr. v. Robins, 447 U.S. 74, 79 (1980) (affirming state supreme court decision upholding state constitutional amendment protecting speech in privately-owned shopping centers, and thereby preventing property owners from excluding certain speakers); Randall Bezanson & Andrew Finkelman, *Trespassory Art*, 43 U. Mich. J.L. Reform 245, 246–47 (2010) (proposing modifications to law of trespass to accommodate new art forms).

[213] *See, e.g.*, United States v. Dierking, No. 08cr3366 JM, 2009 WL 648922, at *1 (S.D. Cal. Mar. 9, 2009) (detailing ongoing prosecution of individual for violation of CFAA in connection with site defacements).

[214] *See, e.g.*, Binary Semantics Ltd. v. Minitab, Inc., No. 4:07-CV-1750, 2008 WL 763575, at *5 (M.D. Pa. Mar. 20, 2008) (finding that the use of a third party's computer to access a website does not prevent a claim under the CFAA).

[215] *See, e.g.*, SEC v. Dorozhko, 574 F.3d 42, 51 (2d Cir. 2009) (finding that although it is unclear that exploiting a weakness in computer code to gain unauthorized access to information is "deceptive" under Securities Exchange Act of 1934, it is entirely possible that computer hacking could be prohibited under the statute).

[216] *See* S. Rep. No. 104-357, at 2 (1996) (amending the CFAA to prohibit specifically violations undertaken "for purposes of commercial advantage or private financial gain").

Likewise, British courts are unlikely to look favorably on methods of hacktivism that seize control of computers and other electronic devices in order either to steal data or to use the devices for some other purpose.[217]

Because certain species of hacktivism do not entail the hijacking of third party systems and are performed without the motive of commercial or financial gain, these forms should not be grouped with those actions that are properly prohibited under the CFAA and the CMA.[218] Thus, primarily expressive forms of hacktivism that do not involve involuntary or unauthorized access and control should be eligible for protection as legitimate means of protest.[219]

3. First, Do No Harm

There is little to commend speech that leaves in its wake material destruction and physical injury.[220] In the context of hacktivism, permissible forms of protest likely to result in actual damage are more readily categorized as conduct rather than expression.[221] Indeed,

---

[217] *See, e.g.*, James Robinson, *Met Must Hand Over News of the World Phone-Hacking Evidence*, GUARDIAN (London) (Mar. 18, 2011), http://www.guardian.co.uk/media/2011/mar/18/met-news-world-hacking-evidence (describing court decision ordering disclosure of evidence gathered in phone-hacking prosecution to plaintiffs in a related civil action).

[218] *Cf.* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 8–10, 12–13.

[219] *Cf. Cantwell*, 310 U.S. at 310 (articulating the First Amendment's requirement that unpleasant and even insulting speech be tolerated); *Edwards*, 372 U.S. at 235 (finding that arrest and conviction of peaceful protestors on charge of breaching the peace "infringed the [protestors'] constitutionally protected rights of free speech, free assembly, and freedom to petition for redress of their grievances"); *Cox*, 379 U.S. at 545 (overturning conviction for breach of the peace on the grounds that no conduct occurred "which the State had a right to prohibit as a breach of the peace").

[220] *See, e.g.*, Feiner v. New York, 340 U.S. 315, 321 (1951) (upholding conviction for disorderly conduct and noting that "[i]t is one thing to say that the police cannot be used as an instrument for the suppression of unpopular views, and another to say that when . . . the speaker passes the bounds of argument . . . and undertakes incitement to riot, they are powerless to prevent a breach of the peace"); Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942) (stating with regard to classes of unprotected or less protected speech, "[i]t has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality"); *Cantwell*, 310 U.S. at 309–10 (noting that "[r]esort to epithets or personal abuse is not in any proper sense communication of information or opinion safeguarded by the Constitution, and its punishment as a criminal act would raise no question under that instrument").

[221] *See, e.g.*, Samuel, *supra* note 24**Error! Bookmark not defined.**, at 8–12 (describing forms of hacktivism like site defacements, site redirects, involuntary DoS attacks, infor-

methods like site redirects, *involuntary* DDoS attacks, information theft and virtual sabotage[222] all feature as primary components *actions* that are both necessary to the method and unambiguously criminal.[223] What is more, the actions in question—namely, hacking computers, web servers, and networks—are largely distinguishable from speech.[224] These forms of hacktivism may be undertaken with a view to expressing some message, but the means involved forfeit any claim for protection.[225]

Like the difference between a legitimate protest and a riot, permissible forms of hacktivism should have as their primary purpose the nonviolent communication of a coherent message.[226] In fact, those forms of hacktivism that do pose a threat of physical damage or violence—i.e., virtual sabotage and other malicious activity—are better described as cyberterrorism.[227] Forms of hacktivism that cause significant monetary harm—as a result of information theft or damage to servers caused by the installation of malware, for example—should likewise be differentiated from hacktivism, and are properly prohibited as cybercrime.[228]

---

mation theft and virtual sabotage that more closely resemble conduct rather than expression).

[222] *See id.* at 11–12 for a description of virtual sabotage.

[223] *See id.* at 10–11.

[224] *See id.* 8–11.

[225] *Cf.* Virginia v. Black, 538 U.S. 343, 365 (2003) (noting distinction between proscribable intimidation and "core political speech" in context of prosecution under state cross burning statute); Spence v. Washington, 418 U.S. 405, 410 (1974) (per curiam) (describing the act of fashioning a peace sign to an American flag as an act of communication protected by the First Amendment); United States v. O'Brien, 391 U.S. 367, 377 (1968) (noting that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms").

[226] *See Tuition Hike Protests: London's Riot vs. Long Beach's "Protest Carnival"*, L.A. Times (Nov. 11, 2010), http://opinion.latimes.com/opinionla/2010/11/tuition-hike-protests-londons-riot-vs-long-beachs-protest-carnival.html. *Compare* Carla Rivera, *Cal State Trustees Approve 15% Tuition Increase*, L.A. Times (Nov. 11, 2010), http://articles.latimes.com/2010/nov/11/local/la-me-calstate-tuition-20101111 (describing "protest carnival" outside California State University Board of Trustees meeting concerning proposed tuition increases), *with* Paul Lewis et al., *Student Protest Over Fees Turns Violent*, Guardian (London) (Nov. 10, 2011), http://www.guardian.co.uk/education/2010/nov/10/student-protest-fees-violent (describing violence surrounding protests in the U.K. over proposals to raise tuition fees and cut funding for university teaching).

[227] *See* Samuel, *supra* note 24**Error! Bookmark not defined.**, at 3, 26.

[228] *See id.* at 28–29.

It does not follow, however, that if *any* harm is caused by an act of hacktivism the act should be considered criminal.[229] It may be that some forms of permissible hacktivism, like virtual sit-ins and voluntary DDoS attacks, do impose some cost on the targets of the protest.[230] In a recent example unrelated to WikiLeaks, a massive DDoS attack against a "non-English blog" on WordPress.com resulted in connectivity problems for other WordPress users.[231] DDoS attacks on Twitter in 2009 caused the site to shut down for several hours, and rendered several of the service's features unusable for some time thereafter.[232] While these attacks were apparently targeted at individual users of both services, their effects had implications for millions of other users.[233] The services themselves likely devoted significant time and resources to defending against and recovering from the attacks.[234] These unfortunate facts alone, however, do not justify criminalizing the attacks.[235]

Protests and demonstrations cause inconvenience, annoyance, and distraction; they can impede commerce and attract unwanted attention.[236] Frequently, they burden the target of the protest and dominate the forum of the demonstration.[237] But, with some exceptions, like the target of a lawful, peaceful demonstration in the physical world, the target of a permissible form of cyberprotest must generally

---

[229] *See id.*

[230] *See, e.g.*, John E. Dunn, *WordPress Recovers From Huge DDoS Attack*, TechWorld (Mar. 4, 2011), http://news.techworld.com/security/3263628/wordpress-recovers-from-huge-ddos-attack/ (describing large DDoS attack on WordPress that resulted in connectivity problems, and attributed the attack to politically-motivated sources targeting a non-English blog on the network); Juan Carlos Perez, *Update: Twitter Still Struggling to Recover from DDoS Attack*, Computerworld (Aug. 7, 2009), http://www.computerworld.com/s/article/9136363/Update_Twitter_still_struggling_to_recover_from_DDoS_attack?taxonomyId=142&pageNumber=1 (describing Twitter's multi-day struggle to restore full services after coming under a strong DDoS attack from an unidentified source).

[231] *See* Dunn, *supra* note 230.

[232] *See* Perez, *supra* note 230; Eliot Van Buskirk, *Denial-of-Service Attack Knocks Twitter Offline*, Wired (Aug. 6, 2009), http://www.wired.com/epicenter/2009/08/twitter-apparently-down/.

[233] *See* Dunn, *supra* note 230; Van Buskirk, *supra* note 232.

[234] *See* Dunn, *supra* note 230; Van Buskirk, *supra* note 232.

[235] *See PruneYard Shopping Ctr.*, 447 U.S. at 87–88.

[236] *See, e.g.*, Robert Mendick & Jason Lewis, *Oxford Graduate Trying to Bring Chaos to Britain's High Streets*, Telegraph (U.K.) (Nov. 13, 2010), http://www.telegraph.co.uk/news/uknews/law-and-order/8131060/Oxford-graduate-trying-to-bring-chaos-to-Britains-high-streets.html (describing protests of companies and storefronts organized via Twitter and Facebook); Economist, *supra* note 185.

[237] *See, e.g.*, Economist, *supra* note 185.

tolerate the inconvenience caused by hacktivism.[238] It is part of the price to be paid for the freedom of expression.[239]

B. *Protest Without Borders*

The burden that must be borne at the site of a protest may be made more tolerable in light of the unique, transnational character of hacktivism.[240] The World Wide Web spans countries and continents, and users are able to share information with a global audience with unprecedented speed. As a result, news of injustice in a previously unreachable locale can be broadcast around the world in an instant.[241] Social media is credited as an important tool for information sharing and organization in the ongoing political unrest in the Middle East.[242] As a result, nonresidents are able to learn of, encourage, and participate in domestic affairs to an extent not possible before the Internet

---

[238] *See PruneYard Shopping Ctr.*, 447 U.S. at 87–88. *But see Frisby*, 487 U.S. at 487–88 (noting that the government may prohibit intrusive speech that is directed at a "captive audience"). It should be noted that the "captive audience" doctrine referenced by the Supreme Court is largely cabined to circumstances in which it is not possible for an onlooker to avert his eyes or otherwise avoid exposure to the offending expression. *Cf.* Lehman v. City of Shaker Heights, 418 U.S. 298, 304 (1974). Such circumstances typically occur in and around a home, car, or public transit. *Cf. Frisby*, 487 U.S. at 487–88; *Lehman*, 418 U.S. at 304. It is less clear that a store's customers or employees would be considered a captive audience. *Cf. PruneYard Shopping Ctr.*, 447 U.S. at 74, 79; Cohen v. California, 403 U.S. 15, 20 (1971) (implying that persons at a courthouse are not a captive audience).

[239] *See Cantwell*, 310 U.S. at 310 (articulating the principle that the First Amendment requires that unpleasant and even insulting speech be tolerated).

[240] *See* Rebekah Denn, *In "Tweets from Tahrir," Twitter Posts Tell the Story of Egypt's Revolution*, Christian Sci. Monitor (Mar. 7, 2011), http://www.csmonitor.com/Books/chapter-and-verse/2011/0307/In-Tweets-from-Tahrir-Twitter-posts-tell-the-story-of-Egypt-s-revolution (describing a book comprised entirely of tweets sent from protestors in Tahrir Square, Cairo, Egypt); Interview by Bob Garfield with Sarah Abdurrahman, Producer, On the Media (Feb. 25, 2011), *available at* http://www.onthemedia.org/transcripts/2011/02/25/01 (describing use of social media by nonresident Libyans to learn about and participate in uprising against authoritarian regime); Molly McHugh, *Libya Inspired by Egyptian Revolution, Uses Social Media in Midst of Protest*, Digital Trends (Feb. 17, 2011), http://www.digitaltrends.com/international/libya-inspired-by-egyptian-revolution-uses-social-media-in-midst-of-protests/ (describing the use of social media to inspire domestic revolution against authoritarian regimes and document violence against civilians).

[241] *See* McHugh, *supra* note 240.

[242] *See id.*

revolution.[243] Using forms of hacktivism as a means of protest, nonresidents are also able to take collective action against injustice.[244]

The upshot is that organizations and governments that were once insulated from criticism by virtue of censorship, oppression or physical distance are now fair game.[245] In countries that restrict Internet access, motivated nonresidents can give voice to dissent that might otherwise go unheard.[246] And where street protests are subject to vicious crackdowns, hacktivism is a reasonably safe means of demonstrating against a regime.[247] Hacktivism can also be a useful tool for communicating complaints against corporations, as Anonymous demonstrated with its attacks during the WikiLeaks episode.[248] Given the multinational nature of many corporations, hacktivism can allow people to register grievances with companies even if the corporate headquarters is located on another continent.[249] In other words, hacktivism offers a tool whereby the object of protest cannot avoid being targeted by virtue of its power or its location, or the poverty or oppression of a people.[250]

Conclusion

As exemplified by Anonymous in the context of the WikiLeaks controversy and the uprisings in the Middle East, hacktivism is increasingly becoming a popular form of protest against perceived injustice. The existing legal regimes at both the international and na-

---

[243] *See, e.g.*, Denn, *supra* note 240; Interview by Bob Garfield, *supra* note 240; McHugh, *supra* note 240.

[244] *See, e.g.*, *Hacktivists Target Egypt and Yemen Regimes*, BBC News (Feb 4, 2011), http://www.bbc.co.uk/news/technology-12364654 (describing actions by members of Anonymous against government websites in Egypt and Yemen); *"Hacktivists" Target Iran's Leadership Online*, Wash. Times (July 1, 2009), http://www.washingtontimes.com/news/2009/jul/01/hacktivism/ (describing hacktivism against web sites belonging to the Iranian government and political leadership); John Leyden, *Anonymous Hacktivists Fire Ion Cannons at Zimbabwe*, Register (Dec. 31, 2010), http://www.theregister.co.uk/2010/12/31/anon_hits_zimbabwe_sites/ (describing hacktivism against web sites belonging to the Zimbabwe government and the ruling political party).

[245] *See supra* text accompanying notes 240–44.

[246] *See id.*

[247] *See Hacktivists Target Egypt and Yemen Regimes*, *supra* note 244; *"Hacktivists" Target Iran's Leadership Online*, *supra* note 244; Leyden, *supra* note 244.

[248] *See supra* text accompanying notes 11–17.

[249] *See id.*

[250] *See Hacktivists Target Egypt and Yemen Regimes*, *supra* note 244; *"Hacktivists" Target Iran's Leadership Online*, *supra* note 244; Leyden, *supra* note 244.

tional levels establish very general categories of prohibited conduct, and courts have not yet squarely addressed the applicability of principles of free speech to laws regulating computer use. This Note has argued that in light of the importance of hacktivism as a legitimate form of protest, courts should interpret laws like the Computer Misuse Act and the Computer Fraud and Abuse Act with the expressive function of hacktivism in mind. Although most current forms of hacktivism are rightly regulated or prohibited outright, a narrow subset of hacktivism should be protected on the grounds that it is primarily expressive, does not involve the hijacking of computers or networks, and causes no significant damage. In addition, the potential for hacktivism as a transnational tool of protest justifies the marginal burden it imposes in its permissible forms.