HACKTIVISM: A NEW BREED OF PROTEST IN A NETWORKED WORLD

NOAH C.N. HAMPSON*

Abstract: After WikiLeaks released hundreds of thousands of classified U.S. government documents in 2010, the ensuing cyber-attacks waged by all sides in the controversy brought the phenomenon of hacktivism into popular focus. Many forms of hacktivism exploit illegal access to networks for financial gain, and cause expensive damage. Other forms are used primarily to advocate for political or social change. Applicable law in most developed countries, including the United States and the United Kingdom, generally prohibits hacktivism. However, these countries also protect the right to protest as an essential element of free speech. This Note argues that forms of hacktivism that are primarily expressive, that do not cause serious damage, and that do not exploit illegal access to networks or computers, sufficiently resemble traditional forms of protest to warrant protection from the application of anti-hacking laws under widely accepted principles of free speech.

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 more than twenty-four hours.[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

* Noah C.N. Hampson is the Editor in Chief of the *Boston College International & Comparative Law Review*. He would like to thank Professor Mary-Rose Papandrea, John Gordon, Lauren Campbell, and Megan Felter for their invaluable advice, assistance, and support.

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

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

[3] *See* Correll, *'Tis the Season*, *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.

attempting to endanger the lives of our troops, 'other assets' & foreign relations #wikileaks #fail."[5]

To get its website 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 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 its content appeared), the WikiLeaks website was once again stable.[10]

The controversy surrounding WikiLeaks, however, was only beginning. Soon, major companies that 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 cardholder

---

[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 & Amazon&st=cse.

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

[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), *available at* 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, denying that the Senator specifically asked Amazon to remove WikiLeaks).

[9] *See* Taylor Barnes, *Booted from U.S.-Based Domain, WikiLeaks Site Finds Refuge with Swiss Pirate Party*, CHRISTIAN SCI. MONITOR (Dec. 3, 2010), *available at* 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/.

payments to WikiLeaks.[13] The next day, Visa did the same.[14] Swiss bank PostFinance closed the account of WikiLeaks founder Julian Assange, claiming that Assange provided false information 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 these corporate announcements sparked an online backlash.[17] An amorphous, international group of individuals, known as "Anonymous," began to bombard the websites of entities it deemed opposed to WikiLeaks with distributed denial of service (DDoS) attacks.[18] Many of the sites crashed, and others were rendered inoperable for some time.[19] The group's declared mission, called Operation Payback, was to raise awareness of the actions of WikiLeaks' opponents, to fight what it perceived to be censorship by identifying and attacking those responsible for the attacks on WikiLeaks, and to support "those who are helping lead our world to freedom and democracy."[20]

To some, the conflict surrounding the WikiLeaks controversy was the first real example of a war over digital information.[21] John Perry Barlow, co-founder of the Electronic Frontier Foundation, announced on Twitter that "[t]he first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops."[22] To others, including members of Anonymous, Operation Payback is the most prominent recent example of a trend that has been developing since the invention of the

---

[13] *See* Declan McCullagh, *MasterCard Pulls Plug on WikiLeaks Payments*, CNET NEWS (Dec. 6, 2010), http://news.cnet.com/8301-31921_3-20024776-281.html.

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

[15] *See* Matthew Allen, *Former WikiLeaks "Bank" Still Denied License*, SWISSINFO.CH (Dec. 21, 2010), 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), 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) [hereinafter Correll, *Payback*], http://pandalabs.pandasecurity.com/operationpayback-broadens-to-operation-avenge-assange/.

[18] *See id.*

[19] *See id.*

[20] *Id.*

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

[22] *Id.*

Internet: computer savvy individuals deploying their skills online to protest for or against a cause—or, more simply, "hacktivism."[23]

Like many aspects of Internet activity, hacktivism is transnational in scope; as a result, any effective legal response should include international coordination that draws on widely accepted democratic principles of free speech.[24] 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 compares the domestic regimes of criminal laws affecting hacktivism in two key signatory states, the United States and the United Kingdom, and it considers how U.S. and UK law protect legitimate protest as a form of free speech, petition, and assembly. 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 protest to warrant protection under widely accepted free speech principles.

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 website defacements, information theft, website parodies, DoS attacks, virtual sit-ins, and virtual sabotage.[25] Capitalizing on the power and pervasive-

---

[23] *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*, H Security (Dec. 9, 2010), http://www.h-online.com/security/news/item/Operation-Payback-protests-via-mouse-click-1150790.html.

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

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

ness of the Internet, hacktivists attempt to exploit its manifold access points to gain publicity and spread information about their views.[26]

Although it has not always carried a clever name, people have turned to hacktivism since the Internet's early days.[27] For example, to protest the passage of the Communications Decency Act of 1996, a hacker defaced the website 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.[28]

Furthermore, as the behavior of The Jester and Anonymous demonstrates, hacktivism is often used by all sides in a debate.[29]

As the Internet has evolved, so too have the tools used by hacktivists to pursue their ideological goals; moreover, an individual's objective and point of view will likely determine his form of hacktivism.[30] Forms of hacktivism run the gamut from those that are clearly covered by existing anti-hacking laws—like redirects, site defacements, and DoS attacks[31]—to forms, like virtual sit-ins, whose legality is far less certain.[32]

B. *Hacktivism versus Hacking*

Although hacktivism has its origins in both hacking and activism,[33] distinguishing between hacktivism and hacking is not straightforward.[34] In one sense, the two practices have divergent motives: hacking is often done out of the hacker's self-interest, while hacktivism is often done to achieve a social or political goal.[35] But the term hacking has not always

---

[26] *See id.* at 5.

[27] *See id.* at 9; Bar-Yosef, *supra* note 23.

[28] Samuel, *supra* note 25, at 9 (citing a copy of a site defacement stored on a mirror site unavailable to the public).

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

[30] *See* Samuel, *supra* note 25 at 8, 48–49.

[31] *See id.* at 49.

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

[33] *See id.* at iii.

[34] *See id.* at 39.

[35] *See id.* at 4.

been used to describe the conduct of a cybercriminal.[36] It originally described an innovative use of technology to solve a problem.[37] In addition, hacking is frequently practiced in defense or furtherance of a unique set of norms that have developed as part of the Internet's culture.[38] For present purposes, however, hacking may be differentiated from hacktivism, in that hacking lacks political objectives.[39]

Much hacking is motivated by nefarious and fraudulent aims.[40] Hackers are responsible for identity theft, fraud, commercial espionage, and other crimes with an annual cost in the trillions of dollars.[41] The FBI has declared that cybercrime is the most significant criminal threat facing the United States, and that anti-cybercrime efforts are a top priority, behind only counterterrorism and counterintelligence.[42]

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.[43] As such, this species of hacking arguably is motivated by political objectives.[44] A major difference from hacktivism, however, is that hacking in cyberwarfare may be analogized to operations on the battlefront, while some forms of hacktivism are more analogous to sit-ins or other forms of nonviolent civil disobedience.[45] 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.[46] Similarly, law enforcement officials fear that cyber-attacks on the networks crucial to the nation's critical infra-

---

[36] *See* Samuel, *supra* note 25, at 39–44.

[37] *See id.* at 51.

[38] *See id.* at 39.

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

[40] *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), *available at* http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

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

[42] *See* Chabinsky, *supra* note 40.

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

[44] *Compare id.*, *with* Samuel, *supra* note 25, at 6.

[45] *Compare* Mueller, *supra* note 43, *with* Samuel, *supra* note 25, at 6.

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

structure—for example, air traffic control systems, electrical grids, and water purification systems—could have even more catastrophic consequences.[47]

By contrast, hacktivism tends to be motivated by political concerns that are at least partly focused on "offline" issues.[48] It is engaged primarily with communicative, not destructive, goals.[49] For example, the defacement of the DOJ website 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.[50] It also reflects the communicative element of hacktivism, in that the website remained largely operational during and after the attack, and the cost of repairing the defacement was minimal.[51]

C. *Forms of Hacktivism*

To analyze 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. It should be noted, though, that as technology evolves, so too will the forms of hacktivism. As a result, the methods described below are merely a sample of hacktivism as it has existed in the recent past; the most popular methods could be very different in the near future. The principles that this Note argues should be applied to determine whether a form of hacktivism ought to receive protection as a legitimate form of protest, however, remain the same.

1. Denial-of-Service Attacks

DoS attacks, the form of hacktivism frequently used during the WikiLeaks incident, involve attempts to block access to websites by any of several means.[52] Access to the targeted site can slow significantly or

---

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

[48] *See* Samuel, *supra* note 25, at 14.

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

[50] *Cf. id.* at 9, 42; *supra* text accompanying note 28.

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

[52] *See* Samuel, *supra* note 25, at 10; Natasha Lomas, *Security from A to Z: DDoS*, CNET NEWS, (Nov. 27, 2006), http://news.cnet.com/Security-from-A-to-Z-DDoS/2100-7349_3-6138447.html?tag=mncol;2n.

be prevented entirely while the attack is underway.[53] During a common type of DoS attack, the party initiating the attack saturates the computer server hosting the target website with requests for information, dramatically increasing the consumption of computational resources and eventually causing the server to slow down or reset.[54]

A popular iteration of the DoS attack is a DDoS attack, which may be distinguished from a DoS attack by its use of a network of multiple attacking computers.[55] 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.[56] 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.[57]

Generally, in order to compromise the security of the infiltrated computer, the virus exploits vulnerabilities in the system.[58] There is no shortage of such vulnerabilities, particularly on home computers and networks.[59] Consequently, botnets are widespread and numerous.[60] In fact, reports suggest that the supply of botnets far exceeds demand, leading to a steep drop in their rental price.[61] With so low a barrier to entry, DDoS capability is proliferating.[62]

Unsurprisingly, DDoS attacks have increased substantially in the past few years.[63] And along with enhanced DDoS capacity has come im-

---

[53] *See* Samuel, *supra* note 25, at 10.

[54] *See Denial of Service Attacks*, CERT SOFTWARE ENGINEERING INST., http://www.cert.org/tech_tips/denial_of_service.html (last visited May 17, 2012).

[55] *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.

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

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

[58] *See* Patrikakis et al., *supra* note 55, at 13.

[59] *See* Geer, *supra* note 24, at xi; McMillan, *supra* note 56.

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

[61] *See id.*

[62] *See id.*

[63] *Compare* Samuel, *supra* note 25, 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 and 2009).

proved and vastly simplified operating software.[64] 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.[65] LOIC allowed users to participate in the attacks in two ways: directly, by entering the target IP address and clicking "fire"; or, alternatively, by volunteering their computer or network to the so-called "LOIC Hivemind," and thereby allowing other users to direct attacks from the surrendered system.[66] The latter option describes a voluntary botnet, in which each computer in the controlled network has effectively been donated for a prescribed use.[67] Unlike members of involuntary botnets, LOIC users retain the ability to add or remove their computers from the attacking network.[68]

Because of the structure of the Internet, DDoS attacks often implicate the laws of multiple nations.[69] An initiating party located in country A can control a network of computers located in countries B, C, and D to attack a website hosted on servers located in country E.[70] Thus, the victim, the evidence, and the perpetrator may be located in different countries, many of which likely have different cybersecurity regimes, or no regime at all.[71]

2. Site Defacements

Site defacements, like that perpetrated against the DOJ website, are believed to be the most common form of hacktivism.[72] 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.[73] Defacements may be limited to a single site, or they may occur in huge volumes across hundreds or thousands of sites.[74] Yet, although

---

[64] *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.

[65] *See id.*

[66] *See id.*

[67] *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/.

[68] *See id.*

[69] *See* Geer, *supra* note 24, at ix.

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

[71] *See* Ryan M.F. Baron, *A Critique of the International Cybercrime Treaty*, 10 COMMLAW CONSPECTUS 263, 270 (2002).

[72] *See* Samuel, *supra* note 25, at 9.

[73] *See id.* at 8.

[74] *See id.* at 9.

they effectively hijack the targeted site in order to communicate a message, defacements do not necessarily damage the targeted site.[75] Instead, site defacements are commonly used not only as a means to communicate a message, but also to demonstrate the technical prowess of the defacer; that is, they are as much about garnering attention for the perpetrator as they are about raising awareness for a cause.[76]

3. Site Redirects

As the name suggests, redirects send users to a site that is different than the one indicated by the web address.[77] 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.[78] Quite often, the alternative site is critical of the original, searched-for site.[79] 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.[80]

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.[81] The difference is that rather than commanding a network of voluntary or involuntary botnets, virtual sit-ins involve individual protestors reloading web pages.[82] Some virtual sit-ins are accomplished simply by users manually and repeatedly reloading the targeted web page; others allow participants to download special code that automatically and repeatedly reloads the targeted site.[83] The virtual sit-in is considered "a mass form of hacktivism . . . [and] a more democratic or representative form of hacktivism."[84]

---

[75] *See id.* at 54.
[76] *See id.* at 55.
[77] *See id.* at 10.
[78] *See* Samuel, *supra* note 25, at 10.
[79] *Id.*
[80] *See id.*
[81] *See id.* at 12.
[82] *See id.*
[83] *See id.* at 12–13.
[84] Samuel, *supra* note 25, at 12.

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.[85] 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.[86]

II. Discussion

The threat posed by hackers has not eluded lawmakers. Indeed, most advanced nations have enacted laws that prohibit hacking.[87] To coordinate international anti-hacking efforts, the 2001 Council of Europe Convention on Cybercrime (Convention) established a framework for domestic legal regimes.[88] The prescribed regimes are general in scope, and could conceivably be applied to forms of hacktivism that resemble traditional forms of protest.[89] The legal systems in the United States and the United Kingdom both feature long established principles and doctrine protective of the freedom of expression.[90] In the context of hacktivism as a form of protest, these doctrines could be used to shield a narrow subset of hacktivism from the general prohibition on hacking.[91]

A. *The European Convention on Cybercrime*

Because its drafters deemed international cooperation critical to effective cybercrime regulation, the Convention prescribes a common criminal policy regarding cybercrime,[92] and signatory parties are bound to establish domestic criminal laws governing intentional acts of cyber-

---

[85] *Id.* at 11.

[86] *See id.* at 123, 137, 143–44.

[87] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006); Computer Misuse Act, 1990, c. 18 (Eng.) (amended 2008), *available at* http://www.legislation.gov.uk/ukpga/1990/18/data.pdf; Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167 [hereinafter Convention].

[88] *See generally* Convention, *supra* note 87.

[89] *See, e.g.*, 18 U.S.C. § 1030; Computer Misuse Act, c. 18 (Eng.).

[90] *See* discussion *infra* Parts II.B–C.

[91] *See* discussion *infra* Part III.

[92] *See* Convention, *supra* note 87, pmbl.

crime.[93] The Convention outlines requirements for substantive laws concerning offenses against the integrity of computer data and systems.[94]

1. Definitions

Article 2 of the Convention requires regulation of illegal access to computer systems.[95] Parties are obligated to enact criminal laws prohibiting access to any part of a computer system "without right."[96] Article 2 specifies that such access may be obtained either by circumventing security measures or by exploiting authorized access to one system to gain unauthorized access to other systems.[97] In addition, parties may require that unlawful access be motivated by intent to obtain computer data or other dishonest intent.[98]

The Convention also requires parties to establish criminal laws prohibiting the intentional, unauthorized interception of computer data. [99] 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 nonpublic transmission.[100] Moreover, the interception of "electromagnetic emissions" from computer systems is prohibited.[101]

Similarly, Articles 4 and 5 respectively require parties to prohibit interference with both data and systems.[102] The Convention provides that data interference may be accomplished when a person intentionally and without authorization damages, deletes, deteriorates, alters, or suppresses computer data.[103] Article 4 states that parties may require that data interference result in serious harm before criminal liability

---

[93] *See id.* 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 71, at 270.

[94] *See id.* § 1.

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

[96] *Id.* art. 2.

[97] *See id.*

[98] *See* Convention, *supra* note 87, art. 2.

[99] *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.* art. 1(b).

[100] *Id.* art. 3.

[101] *Id.*

[102] *See id.* arts. 4, 5.

[103] *Id.* art. 4(1).

attaches.[104] Article 5 obligates parties to prohibit intentional system interference.[105] 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.[106]

In addition to outlining a regime of criminal laws governing data and computer systems, the Convention also describes laws regarding the misuse of devices.[107] Unlike the provisions governing data and computer systems, Article 6 does not impose liability so long as the devices in question are not used to commit offenses set forth in Articles 2 through 5.[108] For devices that are designed or adapted primarily to intercept or interfere with data or systems, however, parties are obligated 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.[109] Furthermore, Article 6 imposes the same restrictions on computer passwords, access codes, and similar information capable of accessing any part of a computer system.[110]

2. Domestic Regimes Prescribed by the Convention

The Convention outlines requirements for domestic laws regarding computer-related offenses.[111] 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.[112] The Article further stipulates that parties are free to condition criminal liability on intent to defraud or other dishonest intent.[113] Relatedly, Article 8 describes antifraud laws to prohibit interference with or manipulation of data or systems that deprive victims of property with the fraudulent intent of procuring an economic benefit for the perpetrator.[114]

---

[104] Convention, *supra* note 87, art. 4(2).
[105] *Id.* art. 5.
[106] *See id.* art. 5.
[107] *See id.* art. 6.
[108] *See id.* art. 6(2).
[109] *Id.*
[110] Convention, *supra* note 87, art. 6(1).
[111] *See id.* tit. 2.
[112] *Id.* art. 7.
[113] *Id.*
[114] *Id.* art. 8.

Finally, the Convention requires parties to establish laws concerning "offences related to infringements of copyright and related rights,"[115] and to establish a legal regime governing ancillary and corporate liability for accessories to cybercrime.[116] 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."[117]

3. Enforcement Provisions of the Convention

The Convention requires parties to establish procedures to allow domestic law enforcement to implement the new laws and investigate and prosecute cybercrimes.[118] It also stipulates that parties must cooperate with each other in the enforcement of cybercrime laws.[119] The Convention describes extradition arrangements that provide for the extradition of suspects from one party state to another to face charges arising from cybercrime laws enacted under the Convention.[120] In addition, the Convention encourages mutual assistance between parties to investigate and prosecute cybercrimes.[121]

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.[122] 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."[123] The Article requires incorporation of the principle of proportionality, and provides that judicial supervision should be given where appropriate.[124] Lastly, Article 15 obligates parties to consider the impact of such laws on the rights and interests of third parties.[125]

---

[115] *Id.* art. 10.
[116] *See* Convention, *supra* note 87, tit. 5.
[117] *See id.* art. 14(2).
[118] *See id.* art. 14(1).
[119] *Id.* art. 23.
[120] *Id.* art. 24.
[121] *Id.* arts. 25, 27–34.
[122] Convention, *supra* note 87, art. 15.
[123] *Id.*
[124] *Id.* art. 15.
[125] *Id.* art. 15(3).

B. *The American Domestic Regime*

1. The Computer Fraud and Abuse Act of 2006

At least forty different federal statutes govern computer-related crimes in the United States.[126] Foremost among these for the regulation of hacking and, potentially, hacktivism, is the Computer Fraud and Abuse Act of 2006 (CFAA).[127] Under the statute, seven categories of conduct are prohibited as they relate to "protected computers," which are defined as:

> [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.[128]

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.[129] Subsection (a)(1) of the statute prohibits obtaining or transmitting classified information through 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.[130] The next subsection prohibits obtaining financial information, information from any government entity, or information from any "protected computer," through unauthorized computer access.[131] Third, the CFAA forbids unauthorized access of any nonpublic computer of the United States government.[132] Subsection (a)(4) proscribes unauthorized computer access with intent to defraud and obtain something of value.[133]

The fifth subsection, § 1030(a)(5), is directed specifically at hacking.[134] The provision describes two distinct types of offenses.[135] The first type involves knowingly transmitting "a program, code or command

---

[126] *See* McCurdy, *supra* note 24, at 300.
[127] 18 U.S.C. § 1030 (2006); *see* McCurdy, *supra* note 24, at 304.
[128] 18 U.S.C. § 1030(e)(2); *see* McCurdy, *supra* note 24, at 304–05.
[129] McCurdy, *supra* note 24, at 304; *see* 18 U.S.C. § 1030(e)(2).
[130] 18 U.S.C. § 1030(a)(1).
[131] 18 U.S.C. § 1030(a)(2).
[132] 18 U.S.C. § 1030(a)(3).
[133] 18 U.S.C. § 1030(a)(4).
[134] *See* 18 U.S.C. § 1030(a)(5); McCurdy, *supra* note 24, at 305.
[135] *See* 18 U.S.C. § 1030(a)(5)(A); McCurdy, *supra* note 24, at 305.

that intentionally causes damage to a protected computer," regardless of whether the actor has authorized access.[136] The second type of offense involves unauthorized access of a protected computer that causes damage.[137] 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.[138]

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 commerce, or if the accessed computer is used by or for the U.S. government.[139] Finally, subsection § 1030(a)(7) prohibits the transmission, with intent to extort, of any communication that threatens to damage a protected computer; to gain unauthorized access to a protected computer and retrieve or impair confidential information; or to extort money in the course of damaging a protected computer.[140]

2. U.S. Courts and the Right to Protest

The distinction between permissible protest and impermissible disruption has been a subject of controversy for generations.[141] 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."[142] 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 not] likely to incite or produce such action."[143] In the context of the First Amendment, contributions to the civic debate on matters of public concern are considered essential to a functioning

---

[136] McCurdy, *supra* note 24, at 305; *see* 18 U.S.C. § 1030(a)(5)(A)(i).

[137] *See* 18 U.S.C. § 1030(a)(5)(A)(ii)–(iii); McCurdy, *supra* note 24, at 305.

[138] *See* 18 U.S.C. § 1030(a)(5)(A)(iii); McCurdy, *supra* note 24, at 305.

[139] 18 U.S.C. § 1030(a)(6).

[140] 18 U.S.C. § 1030(a)(7).

[141] *See, e.g.*, City of Chicago v. Morales, 527 U.S. 41, 56–60 (1999) (striking down city's 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 a criminal conviction arising from the defendant's public desecration of American flag and associated comments he made to an assembled crowd).

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

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

democracy,[144] and the Supreme Court has been extremely reluctant to allow punishment of false or even grievously offensive speech in this area.[145]

The government's ability to limit protest by imposing reasonable time, place, and manner restrictions on speech, however, is largely unquestioned.[146] In this sense, protests can be channeled, but not stifled completely, even if they are peaceful and involve matters of public concern.[147] 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.[148] Such restrictions are permissible even on speech that occurs in areas, like public streets, that traditionally have been used for the exchange of ideas.[149] 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.[150]

---

[144] *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.*

[145] *See id.*; *see also* Snyder v. Phelps, 131 S. Ct. 1207, 1220 (2011) ("[A]s a Nation we have chosen a different course—to protect even hurtful speech on public issues to ensure that we do not stifle public debate."); New York Times Co. v. Sullivan, 376 U.S. 254 *passim* (1964) (overturning jury verdict for defamation against a newspaper for statements published in a full-page issue advertisement concerning the treatment of civil rights protestors by police and state officials).

[146] *See, e.g.*, Frisby v. Shultz, 487 U.S. 474, 487 (1988) (upholding a municipal ordinance specifically prohibiting residential picketing directed at, and occurring in front of, a residence); Police Dep't of Chicago v. Mosley, 408 U.S. 92, 98–99 (1972) (invalidating a municipal anti-picketing ordinance on equal protection grounds, but recognizing the 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 a municipal ordinance prohibiting the use of sound trucks on public streets).

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

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

[149] *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.*

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

The public forum doctrine generally protects speech in "places which by long tradition or by government fiat have been devoted to assembly and debate."[151] In a public forum, the government may impose content-neutral time, place, and manner restrictions.[152] It may also impose a licensing or permit system for the use of public forums so long as the system serves an important purpose, leaves virtually no discretion to the licensing authority, and provides procedural safeguards including judicial review of license denials.[153] Moreover, the public forum doctrine has potential ramifications for speech on private property, if the property is open to the public.[154] It is as yet unclear, however, how, if at all, the Supreme Court will apply the public forum doctrine in the context of the Internet.[155]

C. *The British Domestic Regime*

1. The Computer Misuse Act of 1990

In the United Kingdom, acts of hacktivism generally fall under the Computer Misuse Act of 1990 (CMA).[156] Unlike the American CFAA, the CMA does not define the machines protected by its provisions.[157] Instead, the statute prohibits unauthorized access to "computer material" and defines the actions to which criminal liability will attach.[158] Section 1 provides that a person violates the CMA by knowingly and intentionally gaining unauthorized access to programs or data held in any computer.[159] The provision clarifies the intent requirement by noting that the perpetrator need not intend to gain access to a particular

---

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

[152] *See, e.g.*, Hill v. Colorado, 530 U.S. 703, 714 (2000) (upholding a state law restricting protests outside of health care facilities); Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 289 (1984) (upholding a National Park Service regulation prohibiting sleeping overnight in public parks); Cox v. New Hampshire, 312 U.S. 569, 576 (1941) (affirming convictions for violations of a municipal ordinance requiring a special permit to hold a parade).

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

[154] *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).

[155] *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 to a statute conditioning receipt of federal funds on implementation of filtering software in public libraries).

[156] Computer Misuse Act, c. 18 (Eng.).

[157] *Id.* § 1. *Compare with* 18 U.S.C. § 1030.

[158] Computer Misuse Act, c. 18 (Eng.).

[159] *Id.* § 1(1).

program or data of any kind on any computer; intentionally gaining unauthorized access to the information is sufficient for culpability.[160] The section further states that the maximum sentence of incarceration is two years.[161]

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.[162] Specifically, Section 2 applies to crimes for which there are statutorily fixed sentences or to offenses carrying sentences of five years or more.[163] The further crimes need not occur at the same time as unauthorized access is gained, nor even be possible; the section prohibits arranging for further offenses even if the planned offenses are in fact impossible.[164] The maximum sentence for offenses made in contemplation of further crimes is five years.[165]

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.[166] A person violates Section 3 if he knowingly does "any unauthorized act in relation to a computer."[167] Notably, liability attaches under this section even if the acts are not intentional, but simply reckless.[168]

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.[169] The Section further specifies that acts whose effect is only temporary are nevertheless prohibited, as if the effect was permanent.[170] The maximum sentence under this section is ten years.[171]

Section 3A prohibits making, supplying, or obtaining "articles" to be used in offenses under Sections 1 and 3.[172] "Article" is defined as any

---

[160] *Id.* § 1(2).
[161] *Id.* § 1(3).
[162] *Id.* § 2(1).
[163] *Id.* § 2(2).
[164] Computer Misuse Act, § 2(3)–(4).
[165] *Id.* § 2(5).
[166] *Id.* § 3(2).
[167] *Id.* § 3(1).
[168] *Id.* § 3(4).
[169] *See id.* § 3(4).
[170] *See* Computer Misuse Act, § 3(5)(c).
[171] *Id.* § 3(6).
[172] *Id.* § 3A.

program or data held in electronic form.[173] 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 violates Sections 1 or 3.[174] Violations under Section 3A are punishable by a maximum sentence of two years.[175]

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,"[176] 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.[177] Section 5 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.[178]

2. British Courts and the Right of Expression

In the United Kingdom, free speech receives less robust protection than in the United States.[179] 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."[180] Judicial review of laws restricting speech is largely nonexistent; the freedom of speech is protected nearly exclusively by parliamentary "self-control."[181] The United Kingdom does not have a written constitution, and the only textual protection for speech rights is the Human Rights Act of 1998 (HRA),[182] which codifies, among other things, Article 10 of

---

[173] *Id.* § 3A(4).

[174] *Id.* § 3A(2).

[175] *Id.* § 3A(5).

[176] Computer Misuse Act, § 4(2).

[177] *Id.* § 4(1).

[178] *Id.* § 5(2)–(3).

[179] *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 of 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 the British government's direct broadcast ban for organizations in Northern Ireland thought to support terrorism).

[180] *See, e.g.*, KROTOSZYNSKI, *supra* note 179, at 187.

[181] *Id.* at 187–88.

[182] *Id.* at 184.

the European Convention for the Protection of Human Rights and Fundamental Freedoms.[183]

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.[184] British courts frequently have invoked the common law principle to cabin laws that would otherwise inhibit the exercise of free speech.[185] In libel cases, for example, British courts have formulated fair comment and privilege defenses that protect speech.[186] Common law principles of free speech have also been invoked to limit the scope of legislation that could have restricted speech rights.[187]

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.[188] 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.[189] As a result, the principle of free speech in the United Kingdom remains comparatively limited at common law.[190]

III. Analysis

A. *Hacktivism as Legitimate Protest*

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

---

[183] *See id.* at 183. Article 10 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.* art. 10(2).

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

[185] *See id.* at 40.

[186] *See id.*

[187] *See id.* at 41.

[188] *See id.* at 41–42.

[189] *See id.* at 42.

[190] *Cf. id.* at 41–42.

that cause little or no permanent damage, should receive at least some protection as a legitimate form of protest. As an initial matter, to carve out protection for hacktivism in the existing international anti-hacking legal regime, it is necessary to distinguish between harmful, and thus rightly prohibited, forms of hacking, and types of hacktivism that are primarily expressive, do not exploit illegal access to networks and computers, and do not cause serious damage.[191] Unsurprisingly, this is easier said than done.[192]

Just as traditional means of protest can inconvenience and frustrate both the object of the protest and the general public, hacktivism, too, can often seem more like a nuisance than an exercise of protected rights of expression.[193] And the unique forum of online protest—cyberspace, which exists on privately owned servers, and yet functions as a global public square[194]—further complicates the question of whether the Internet is an appropriate situs for demonstration.[195] Nevertheless, the same democratic interests that require toleration of civil demonstration in the physical world demand that a narrow subset of hacktivism be protected as a legitimate form of political protest.[196] Given that hacktivism may take a wide variety of forms,[197] to separate the "good" hacktivism from the "bad," it is useful first to establish some parameters.

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-

---

[191] *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.

[192] *See* 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/; *WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, *supra* note 191.

[193] *See WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, *supra* note 191.

[194] *Cf.* James Grimmelmann, *The Internet Is a Semicommons*, 78 FORDHAM L. REV. 2799, 2799–800 (2009) (describing the public nature of the communications that flow through the Internet, despite the private infrastructure used to support the network).

[195] *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/.

[196] *See WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, *supra* note 191.

[197] *See* Samuel, *supra* note 25, at 7.

vate property.[198] Even in the United States, where speech rights are heavily guarded by the First Amendment, not all expression receives protection.[199] Hacktivism that causes damage (for example, information theft) or involves the manipulation of hijacked private property (for example, DDoS attacks using involuntary botnets) therefore is not likely to be considered expression at all.[200]

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.[201] 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 websites as a source of vital information, restrictions on otherwise permissible cyberprotests are likely in many circumstances.[202] For example, virtual sit-ins waged against the official website of an incumbent political officeholder that

---

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

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

[200] *See, e.g.*, Charlie Savage, *Soldier Faces 22 New WikiLeaks Charges*, N.Y. TIMES, Mar. 2, 2011, at A6; 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).

[201] *See, e.g.*, Frisby v. Shultz, 487 U.S. 474, 487 (1988) (upholding a municipal ordinance specifically prohibiting residential picketing directed at, and occurring in front of, a residence); Police Dep't of Chicago v. Mosley, 408 U.S. 92, 98–99 (1972) (invalidating a municipal anti-picketing ordinance on equal protection grounds, but recognizing the 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 a municipal ordinance prohibiting the use of sound trucks on public streets).

[202] 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 a municipal ordinance prohibiting the display of yard signs on private property), Martin v. City of Struthers, 319 U.S. 141, 146–47 (1943) (invalidating a municipal ordinance prohibiting door-to-door distribution of handbills), *and* Schneider v. State, 308 U.S. 147, 162 (1939) (invalidating a municipal anti-leafleting ordinance), *with* Heffron v. Int'l Soc'y for Krishna Consciousness, 452 U.S. 640, 651 (1981) (upholding a state regulation prohibiting the sale or distribution of merchandise and literature at the state fair, except from a booth rented from the state, on grounds that the state had sufficiently substantial interest in regulating solicitation activities at fairgrounds), Greer v. Spock, 424 U.S. 828, 838 (1976) ("[T]he 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) ("[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.").

might be otherwise protected could conceivably be prohibited in the period leading up to an election.[203] Or, while a virtual sit-in by students on the website 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 website of the high school newspaper could be punished on the theory that the state has a substantial interest in controlling the terms of debate within secondary schools.[204] 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.[205]

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 HRA.[206] In the context of the

---

[203] *Cf.* City Council of L.A. v. Taxpayers for Vincent, 466 U.S. 789, 807–08 (1984) (upholding a municipal regulation prohibiting the posting of 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, 898 (2010) (striking down on First Amendment grounds limits on campaign expenditures by corporations).

[204] *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 be endorsed by the school); Bethel Sch. Dist. v. Fraser, 478 U.S. 675, 683 (1986) (upholding the punishment of a high school student for vulgar speech given in a 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 a state university violated the 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).

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

[206] *See* BARENDT, *supra* note 184, at 43 (noting that while the HRA incorporates the guarantee of the right of free expression in Article 10 of the ECHR, it is not clear what functions are encompassed by the clause); KROTOSZYNSKI, *supra* note 179, at 190 ("[Although] British

WikiLeaks controversy, this premise will almost certainly be tested in the near future as members of Anonymous have "declared war" on the British government.[207] 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.[208] Given the British courts' wide discretion in applying common law principles to statutory interpretation, and in light of the uncertainty surrounding the interpretation of the HRA,[209] as such attacks proliferate it is likely that various types of hacktivism will be prosecuted.[210]

It would not be surprising if British courts refused to recognize a free speech exception to the CMA for hacktivism, even under the HRA.[211] There is some precedent, however, that might support finding that punishing certain forms of hacktivism would infringe speech rights.[212] But recent trends suggest that at least in the near future, the British government may be increasingly inclined to suppress protest.[213]

---

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.").

[207] 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.

[208] *Id.*

[209] *See* BARENDT, *supra* note 184, at 41–42 (explaining that common law presumptions require a balancing of speech rights against other rights that may weigh against free speech).

[210] *See* Taylor, *supra* note 207 (noting criticism of British government's cybersecurity preparedness and vulnerability to DDoS attacks in light of threat of mass cyberprotests).

[211] *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 179, 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").

[212] *See, e.g.*, Brutus v. Cozens, [1973] A.C. 854 (H.L.) 863 (U.K.) (affirming dismissal of charges of using insulting behavior); 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 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." Therefore, "vigorous and . . . 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.

[213] *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

In the case of Anonymous' DDoS attacks, government crackdowns have already begun.[214] Whether or not the courts or Parliament will recognize these attacks as a protectable form of expression is yet to be seen.[215]

To the extent that an act of hacktivism is expressive, however, it should be eligible for protection as a form of legitimate protest.[216] 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.[217] 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 protection, so too should acts of hacktivism that are primarily expressive receive protection.[218]

2. Hacktivism, not Hijacking

Although the U.S. 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

---

proposal to request a ban on street marches if violence associated with ongoing protests does not subside).

[214] *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).

[215] *See id.* (describing the discretion given to police to prohibit street demonstrations); *supra* text accompanying notes 179–189 (describing limited textual protection for free expression and discretion granted to courts and Parliament to restrict speech in favor of other interests).

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

[217] *See* Taylor, *supra* note 207 ("[T]he 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 67 (describing the 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 Tucson 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 a sit-in at a U.S. senator's office in protest of senator's immigration policies, and noting senator's acknowledgment of the protestors' right to peacefully protest).

[218] *See* Cox v. Louisiana, 379 U.S. 536, 546, 547 (1965) (overturning conviction for breach of the peace on the grounds that the State's prohibition on certain conduct as a breach of the peace was unconstitutional); 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' First Amendment rights); Cantwell v. Connecticut, 310 U.S. 296, 310 (1940) (articulating the principle that the First Amendment requires toleration of unpleasant and even insulting speech).

forms of hacktivism.[219] Website defacements, for example, are unlikely to be protected, in part because they involve hacking into web servers and replacing the owners' content.[220] 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.[221] And it should go without saying that acts like information theft will almost invariably be condemned under any statute.[222] The same is true of acts that are undertaken with a view to obtaining commercial or financial advantage.[223]

Likewise, British courts are unlikely to look favorably on methods of hacktivism that seize control of computers and other electronic devices either to steal data or to use the devices for some other purpose.[224] 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.[225] Thus, primarily expressive forms of hacktivism that do not involve involuntary or unauthorized access and control, like virtual sit-ins and

---

[219] *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).

[220] *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).

[221] *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).

[222] *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).

[223] *See* S. REP. No. 104-357, at 2 (1996) (amending the CFAA to prohibit specifically violations undertaken for commercial or financial advantage).

[224] *See, e.g.*, James Robinson, *Met Must Hand over News of the World Phone-Hacking Evidence*, GUARDIAN (U.K.) (Mar. 18, 2011), *available at* 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).

[225] *Cf.* Samuel, *supra* note 25, at 8–10, 12–13.

voluntary DDoS attacks, should be eligible for protection as legitimate means of protest.[226]

3. Hacktivism Without Harm

There is little to commend speech that leaves in its wake material destruction and physical injury.[227] In the context of hacktivism, permissible forms of protest likely to result in actual damage are more readily categorized as conduct rather than expression.[228] Indeed, methods like site redirects, involuntary DDoS attacks, information theft and virtual sabotage[229] all feature as primary components *actions* that are both necessary to the method and unambiguously criminal.[230] What is more, the actions in question—namely, hacking computers, web servers, and networks—are largely distinguishable from speech.[231] These forms of hacktivism may be undertaken with a view to expressing some message, but the means involved forfeit any claim for protection.[232]

---

[226] *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' First Amendment rights); *Cox*, 379 U.S. at 545 (overturning conviction for breach of the peace on the grounds that the State's prohibition on certain conduct as a breach of the peace was unconstitutional).

[227] *See, e.g.*, Feiner v. New York, 340 U.S. 315, 321 (1951) ("It 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) ("It 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 ("Resort 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.").

[228] *See, e.g.*, Samuel, *supra* note 25, at 8–12 (describing forms of hacktivism like site defacements, site redirects, involuntary DoS attacks, information theft, and virtual sabotage that more closely resemble conduct rather than expression).

[229] *See id.* at 11–12.

[230] *See id.* at 10–11.

[231] *See id.* 8–11.

[232] *Cf.* Virginia v. Black, 538 U.S. 343, 365 (2003) (noting the distinction between proscribable intimidation and "core political speech" in the 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) ("[W]hen '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.").

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.[233] In fact, those forms of hacktivism that do pose a threat of physical damage or violence—that is, virtual sabotage and other malicious activity—are better described as cybercrime or cyberterrorism.[234] 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.[235]

It does not follow, however, that if *any* harm is caused by an act of hacktivism, the act should be considered criminal.[236] 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.[237] 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.[238] In another example, 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.[239] While these attacks were apparently targeted at individual

---

[233] *See* Op-Ed., *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 (U.K.) (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).

[234] *See* Samuel, *supra* note 25, at 3, 26.

[235] *See id.* at 28–29.

[236] *See id.*

[237] *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 attributing 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 (describing Twitter's multi-day struggle to restore full services after coming under a strong DDoS attack from an unidentified source).

[238] *See* Dunn, *supra* note 237.

[239] *See* Eliot Van Buskirk, *Denial-of-Service Attack Knocks Twitter Offline*, WIRED (Aug. 6, 2009), http://www.wired.com/epicenter/2009/08/twitter-apparently-down/; Perez, *supra* note 237.

users of both services, their effects had implications for millions of other users.[240] The services themselves likely devoted significant time and resources to defending against and recovering from the attacks.[241] These unfortunate facts alone, however, do not justify criminalizing the attacks.[242]

Protests and demonstrations cause inconvenience, annoyance, and distraction; they can impede commerce and attract unwanted attention.[243] Frequently, they burden the target of the protest and dominate the forum of the demonstration.[244] 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 tolerate the inconvenience caused by hacktivism.[245] It is part of the price to be paid for the freedom of expression.[246]

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.[247] The World Wide Web spans countries and continents,

---

[240] *See* Dunn, *supra* note 237; Van Buskirk, *supra* note 239.

[241] *See* Dunn, *supra* note 237; Van Buskirk, *supra* note 239.

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

[243] *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); *WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, *supra* note 191.

[244] *See, e.g.*, *WikiLeaks, Protest and the Law: The Rights and Wrongs of Hacktivism*, *supra* note 191.

[245] *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).

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

[247] *See* 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); 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/

and users are able to share information with a global audience with unprecedented speed. News of injustice in a previously unreachable locale can be broadcast around the world in an instant.[248] Social media is credited as an important tool for information sharing and organization in the ongoing political unrest in the Middle East.[249] As a result, nonresidents are able to learn of, encourage, and participate in domestic affairs to an extent not possible before the Internet revolution.[250] Using forms of hacktivism as a means of protest, nonresidents are also able to take collective action against injustice.[251]

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.[252] In countries that restrict Internet access, motivated nonresidents can give voice to dissent that might otherwise go unheard.[253] And where street protests are subject to vicious crackdowns, hacktivism is a reasonably safe means of demonstrating against a regime.[254] Hacktivism can also be a useful tool for communicating complaints against corporations, as Anonymous demonstrated with its attacks during the WikiLeaks episode.[255] Given that many corporations

---

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); 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).

[248] *See* McHugh, *supra* note 247.

[249] *See id.*; *see also* Sarah Joseph, Essay, *Social Media, Political Change, and Human Rights*, 35 B.C. INT'L & COMP. L. REV. 145, 166–67 ("[T]here is little doubt that the 'weak activist' tool of social media has been used in the Arab world by a loose network of people to encourage or facilitate their taking of very great risks.").

[250] *See, e.g.*, Interview by Bob Garfield, *supra* note 247; Denn, *supra* note 247; McHugh, *supra* note 247.

[251] *See, e.g.*, 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 websites belonging to the Zimbabwe government and the ruling political party); *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 websites belonging to the Iranian government and political leadership).

[252] *See supra* text accompanying notes 240–244.

[253] *See supra* text accompanying notes 240–244.

[254] *See* Leyden, *supra* note 251; *Hacktivists Target Egypt and Yemen Regimes*, *supra* note 251; *"Hacktivists" Target Iran's Leadership Online*, *supra* note 251.

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

are multinational, hacktivism can allow people to register grievances with companies even if the corporate headquarters are located on another continent.[256] 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 a people's poverty or oppression.[257]

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 national 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. In addition, the potential for hacktivism as a transnational tool of protest justifies the marginal burden it imposes in its permissible forms. 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.

---

[256] *See id.*

[257] *See* Leyden, *supra* note 251; *Hacktivists Target Egypt and Yemen Regimes*, *supra* note 251; *"Hacktivists" Target Iran's Leadership Online*, *supra* note 251.