Harvard Journal of Law & Technology
Volume 27, Number 1 Fall 2013

HACKTIVISM AND THE FIRST AMENDMENT: DRAWING THE LINE BETWEEN CYBER PROTESTS AND CRIME

*Xiang Li**

TABLE OF CONTENTS

---

* Harvard Law School, J.D., *magna cum laude*, 2013. Associate, Morrison & Foerster LLP. Special thanks to Professor Mark Tushnet for his generosity in advising the paper that led to this Note, and to Andy Sellars and Sarah Duran for their insightful comments. I would also like to thank Article Editor Spencer Haught, Michael Qin, and the staff of the *Harvard Journal of Law & Technology* for their hard work in bringing this Note to print. All errors remain my own.

I. INTRODUCTION

The Digital Revolution has given rise to a "new kind of society . . . shaped by computing . . . ."[1] The worldwide web turns twenty-two this year,[2] and virtual technology now extends many of our daily and originally "analog" activities, from consumption to social interaction, into cyberspace.

Reflecting these changes, a new form of digital activity — hacktivism — has taken root in the online environment. Although a lexical debate persists over the treatment and content of the term, in its simplest and broadest sense, it involves the use of technology hacking mechanisms, often in the form of cyberattacks,[3] to effect particular political and/or social change.[4] Hacktivism first emerged in the

1. Editorial, *Digital Revolution: Time to Question Our Love Affair with New Tech*, GUARDIAN (Mar. 9, 2013), http://www.guardian.co.uk/commentisfree/2013/mar/10/new-technology-bleak-or-brave.

2. *Id.*

3. Although the term "cyberattack" is commonly used to refer to all forms of online intrusion into the target website, some commentators distinguish between cyberattacks, which "alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks," and "cyber exploitations, which are non-destructive actions that extract confidential information." Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 439–40 (2012) (citations omitted) (internal quotation marks omitted). Given that hacktivists often use cyberattacks in conjunction with cyber exploitations, this Note uses the term "cyberattacks" as it is broadly understood. *See, e.g.*, Mathew J. Schwartz, *Anonymous Posts Westboro Church Members' Personal Information*, INFO. WEEK (Dec. 18, 2012, 3:01 PM), http://www.informationweek.com/security/privacy/anonymous-posts-westboro-church-members/240144592 (discussing Anonymous's use of distributed denial-of-service ("DDoS") attacks as well as hacking that uncovered personal information of members of the Westboro Baptist Church).

4. *See* Peter Ludlow, *What is a 'Hacktivist'?*, N.Y. TIMES OPINIONATOR BLOG (Jan. 13, 2013, 8:30 PM), http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist (noting that the untimely death of Aaron Swartz has reheated the lexical warfare over the term "hacktivism" as commentators argue over "whether Swartz's activities as a 'hacktivist' were being unfairly defined as malicious or criminal"). *See infra* Section II for a discussion of the definition and forms of hacktivism.

1990s,[5] and the use of cyberattacks has proliferated in recent years, spawning no shortage of headlines.[6]

For instance, since 2008, the loosely associated hacktivist group called Anonymous has launched numerous cyberattacks to support various political and social causes.[7] The targets of Anonymous have ranged from corporate[8] to government[9] to religious entities.[10] The triggers for the attacks have been manifold, including: corporate censorship of WikiLeaks, prosecutorial overreach in the case of Aaron Swartz, and planned picketing by Westboro Baptist Church at the funerals of Sandy Hook Elementary School victims.[11]

---

5. TIM JORDAN & PAUL TAYLOR, HACKTIVISM AND CYBERWARS: REBELS WITH A CAUSE? 5 (2004); Seth F. Kreimer, *Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet*, 150 U. PA. L. REV. 119, 156 (2001).

6. *See, e.g.*, *Recent Cyber Attacks*, FORBES, http://www.forbes.com/pictures/mhl45gkeg/sony-2 (last visited Dec. 20, 2013); Paul Roberts, *Verizon: Hacktivists Steal Most Data in 2011*, THREAT POST (Mar. 22, 2012, 3:59 AM), http://threatpost.com/verizon-hacktivists-steal-most-data-2011-032112/76350. For a historical account of the emergence of hacktivism, see, e.g., Ty McCormick, *Hacktivism: A Short History*, FOREIGN POL'Y (Apr. 29, 2013), http://www.foreignpolicy.com/articles/2013/04/29/hacktivism.

7. *See* Cassell Bryan-Low & Siobhan Gorman, *Inside the Anonymous Army of 'Hacktivist' Attackers*, WALL ST. J., June 23, 2011, at A1, *available at* http://online.wsj.com/article/SB10001424052702304887904576399871831156018.html. Anonymous grew out of an online message forum created in 2003, which attracted hackers and gamers "fond of mischievous pranks." *Id.* In 2008, as Anonymous members became more politically focused, the group began a campaign against the Church of Scientology, which involved DDoS attacks and helped Anonymous gain public awareness. *See id.* Since 2008, Anonymous has played such a prominent role in cyberattacks that a recent survey shows sixty-one percent of IT security professionals are concerned about attacks from Anonymous or other hacktivists. Steve Ragan, *Bit9 Survey: InfoSec Professionals Concerned about Anonymous*, SECURITY WEEK (Apr. 23, 2012), http://www.securityweek.com/bit9-survey-infosec-professionals-concerned-about-anonymous.

8. *See, e.g.*, Ryan Singel, *Vigilantes Take Offensive in WikiLeaks Censorship Battle*, WIRED (Dec. 8, 2010, 5:42 PM), http://www.wired.com/threatlevel/2010/12/pro-wikileaks-vigilantes-down-visa-com (describing cyberattacks launched by Anonymous against websites of banking companies that withdrew service from WikiLeaks).

9. *See, e.g.*, Violet Blue, *Feds Stumbling After Anonymous Launches 'Operation Last Resort,'* ZDNET (Jan. 30, 2013, 11:34 AM), http://www.zdnet.com/feds-stumbling-after-anonymous-launches-operation-last-resort-7000010541/ (describing cyberattacks launched by Anonymous against federal government websites to protest the prosecution of Aaron Swartz).

10. *See, e.g.*, Walter Pavlo, *Anonymous' Hackers Target Westboro Baptist Church After Protest Plans*, FORBES (Dec. 18, 2012, 7:32 PM), http://www.forbes.com/sites/walterpavlo/2012/12/18/anonymous-hackers-target-westboro-baptist-church-after-protest-plans (describing cyberattacks launched by Anonymous against members of Westboro Baptist Church to deter protests at the funerals of Sandy Hook Elementary School victims).

11. *See supra* notes 8–10. Outside of the domestic context, Anonymous has also launched attacks against foreign governments, most recently against the North Korean government for its warmongering rhetoric. *'Anonymous Korea' Claim Taking Down N.Korean Govt Websites*, RUSSIA TODAY (Mar. 30, 2013, 8:36 AM), http://rt.com/news/anonymous-korea-tango-attack-085, and the Burmese government for its persecution of the Rohingya people, *Anonymous Targets Genocide in Myanmar (Burma): Operation Rohingya*, EXAMINER (Mar. 25, 2013), http://www.examiner.com/article/anonymous-targets-genocide-myanmar-burma-operation-rohingya.

On January 7, 2013, Anonymous submitted a "We the People" petition asking the White House to recognize distributed denial-of-service ("DDoS") attacks[12] as a valid form of protest protected by the First Amendment.[13] Anonymous analogized DDoS attacks to physical "Occupy" encampments, arguing that protestors are similarly "occupying" a particular webpage through the use of repeated refreshes to delay or deny access to that virtual location for a finite period of time.[14] Consistent with Anonymous's position, some commentators argue that hacktivism amounts to digital civil disobedience, whether achieved through the mechanism of disruption (e.g., DDoS attacks), information distribution (e.g., hacking and leaking), or otherwise.[15]

Does hacktivism constitute a legitimate instrument of protest in twenty-first century America? This Note examines the viability of invoking the First Amendment as a defense to the prosecution of hacktivism, specifically in the form of cyberattacks, under the Computer Fraud and Abuse Act ("CFAA").[16] Although existing forms of cyberattacks are unlikely to merit First Amendment protection, this Note argues that hacktivism may evolve over time to fall within the purview of First Amendment protection. A categorical prohibition on all forms of hacktivism may sweep up socially productive uses of cyberattacks as a form of protest.

The argument proceeds in four parts. Section II describes the various forms of cyberattacks currently used by hacktivists, as well as the potential criminal liability for hacktivism under the CFAA. Section III examines the primary obstacle to, and secondary arguments against, invoking First Amendment protections for hacktivism as free speech. Section IV presents two of the central premises underlying the rise of hacktivism and discusses the need to reconceptualize what is currently

---

12. *See infra* note 22 and accompanying text (defining a DDoS attack as overwhelming a target website's server with repeated requests from multiple computers).

13. Mike Masnick, *Anonymous Launches White House Petition Saying DDoS Should Be Recognized As A Valid Form Of Protest*, TECHDIRT (Jan. 11, 2013, 7:39 PM), http://www.techdirt.com/articles/20130111/08053821642/anonymous-launches-white-house-petition-saying-ddos-should-be-recognized-as-valid-form-protest.shtml. The petition failed to meet the threshold number of signatures required to guarantee a White House response. *See Make, distributed denial-of-service (DDoS), a legal form of protesting*, WHITEHOUSE.GOV, https://petitions.whitehouse.gov/petition/make-distributed-denial-service-ddos-legal-form-protesting/X3drjwZY (last visited Dec. 20, 2013) ("The petition you are trying to access has expired, because it failed to meet the signature threshold.").

14. Masnick, *supra* note 13.

15. *See, e.g.*, Evgeny Morozov, *In Defense of DDoS*, SLATE (Dec. 13, 2010, 6:30 PM), http://www.slate.com/articles/technology/technology/2010/12/in_defense_of_ddos.html; Michael Scherer, *The Geeks Who Leak*, TIME (June 24, 2013), http://content.time.com/time/magazine/article/0,9171,2145506-1,00.html; *Hacktivists: Heroes Or, Well, Hacks?*, NPR (June 13, 2013, 12:00 PM), http://www.npr.org/templates/story/story.php?storyId=191316143. *But see* Joshua McLaurin, Note, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 237–47 (2011) (discussing the flawed comparison between hacktivism and civil disobedience).

16. 18 U.S.C. § 1030 (2012).

a privatized cyberspace to make room for public forums that can provide specific access to a target's online property. Additionally, Section IV discusses the possible evolution of hacktivism to include cyberattacks that generate pop-up windows to communicate protest messages.[17] Such a mechanism could raise the possibility of First Amendment protection whereby the cyberattack constitutes protected speech and the pop-up window qualifies as a public forum, akin to a "cyber sidewalk" adjacent to the target's online property. Section V concludes.

II. HACKTIVISM AND CRIMINAL LIABILITY

A. Hacktivism: Political Protest Gone Electronic?

1. What Is Hacktivism?

Although "hacktivism" is a loaded term that elicits mixed responses to its legitimacy, hacktivism can be broadly defined as the "combination of grassroots political protest with computer hacking"[18] through the "nonviolent use of illegal or legally ambiguous digital tools [to pursue] political ends."[19] In her dissertation, Alexandra Samuel presented the following matrix framework to help locate hacktivism along a spectrum of online and offline forms of political protest and activism:[20]

17. *Pop-Up*, WHATIS.COM, http://whatis.techtarget.com/definition/pop-up (last updated Apr. 05, 2005).

18. TIM JORDAN & PAUL TAYLOR, HACKTIVISM AND CYBERWARS: REBELS WITH A CAUSE? 1 (2004) ("Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilising virtual powers to mould offline life . . . . Hacktivism is activism gone electronic.").

19. Alexandra Whitney Samuel, Hacktivism and the Future of Political Participation, 2 (Sept. 2004) (unpublished Ph.D. dissertation, Harvard University), *available at* http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf; *accord* Robert Vamosi, *How Hacktivism Affects Us All*, PC WORLD (Sept. 6, 2011, 6:30 PM), http://www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html.

20. Samuel, *supra* note 19, at 6–7 tbl.1.

Table 1: Spectrum of Online and Offline Forms of Activism

	Offline	**Online**
Conventional	**Activism:** Voting Electioneering Non-violent protest marches Boycotts	**Online activism:** Online voting Online campaign donations Online petitions
Transgressive	**Civil disobedience:** Sit-ins Barricades Political graffiti Wildcat strikes Underground presses Political theater Sabotage	**Hacktivism:** Website defacements Website redirects Denial-of-service attacks Information theft Site parodies Virtual sabotage Software development
Violent	**Terrorism:** Political bombing Political hijacking Tree spiking	**Cyberterrorism:** Hacking air traffic control Hacking power grid (*note: to date these examples are purely hypothetical*)

Hacktivism can either be directed at the target's online property in the form of a cyberattack, as with DDoS attacks, or it can develop independently of the target's online property, as with website parodies.[21] This Note confines its First Amendment analysis to cyberattacks.

a. Forms of Cyberattacks

Cyberattacks can take a variety of different forms, which can be difficult to define in light of constantly changing technology. To avoid this problem, the following descriptions seek to distinguish categories of cyberattacks based on their *effects*, rather than the technologies they employ:

1. Website unavailability: A target website can (1) become unavailable because the server is overwhelmed with traffic, or (2) *effectively* become unavailable because the cyberattack redirects traffic to an alternative website. For example, a DDoS attack involves overwhelming a target website's server with repeated requests from multiple computers.[22] With enough volume,[23] repeated requests will

21. *See id.* at 12–13.

22. Kesan & Hayes, *supra* note 3, at 444. For a visual illustration explaining the recent DDoS attack against a European spam-prevention service, see Alan McLean et al., *How the*

cause the server to slow down or crash, thereby rendering the target website unable to load.[24] DDoS attacks are often performed through the use of many involuntarily co-opted computers in the form of botnets,[25] or through the use of software allowing for voluntary participation in DDoS attacks.[26] For example, in Operation Payback, Anonymous used DDoS attacks to take down the websites of Mastercard and Visa.[27] Anonymous initiated these attacks in response to the credit card companies' decisions to terminate services to WikiLeaks following the site's public release of U.S. diplomatic cables.[28] Alternatively, a cyberattack can involve hacking into the web server and altering the address settings to redirect visitors to a different website.[29] For example, cyberattacks against media company Al Jazeera redirected visitors to a webpage with the Syrian flag and a message criticizing the company for its "stand against Syria . . . and [its] support for militant terrorism."[30]

2. Content alteration: Cyberattacks can deface the target website by hacking into the server and replacing or altering the target webpage(s) with other content.[31] For example, Operation Last Resort, launched by Anonymous to avenge Aaron Swartz, involved defacing the U.S. Sentencing Commission's website with a message detailing the group's grievances against the federal sentencing guidelines.[32]

Cyberattack on Spamhaus Unfolded, N.Y. TIMES (Mar. 30, 2013), http://www.nytimes.com/interactive/2013/03/30/technology/how-the-cyberattack-on-spamhaus-unfolded.html.

23. *See* McLaurin, *supra* note 15, at 217 ("[T]he outcome of an attack depends in large part on the . . . resources available to the target. Target servers with larger bandwidth and more data ports for opening connections with other computers will fare better on average, since a successful attack must deplete one of those resources.").

24. Noah C.N. Hampson, Note, *Hacktivism: A New Breed of Protest in a Networked World*, 35 B.C. INT'L & COMP. L. REV. 511, 517–18 (2012), *available at* http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr; McLaurin, *supra* note 15, at 212.

25. Botnets are a collection of Internet-connected programs communicating with each other to perform related tasks. Such programs may be malicious, allowing a hacktivist to take control of the infected computer. McLaurin, *supra* note 15, at 217.

26. For example, the Low Orbit Ion Cannon is an open-source application developed to allow users without the technical know-how to participate in DDoS attacks. Joel Johnson, *What Is LOIC?*, GIZMODO (Dec. 8, 2010, 5:20 PM), http://gizmodo.com/5709630/what-is-loic.

27. *See* Singel, *supra* note 8.

28. *See id.*

29. Hampson, *supra* note 24, at 520; Samuel, *supra* note 19, at 10.

30. *Hackers Target Al Jazeera Websites*, AL JAZEERA, http://www.aljazeera.com/news/middleeast/2012/09/20129510472158245.html (last modified Sept. 5, 2012, 12:33 PM).

31. Samuel, *supra* note 19, at 8.

32. Martyn Williams, *Hacker Collective Anonymous Hits US Government Site*, PC WORLD (Jan. 27, 2013, 3:36 AM), http://www.pcworld.com/article/2026500/hacker-collective-anonymous-hits-us-government-site.html. The message began with:

> This website was chosen due to the symbolic nature of its purpose — the federal sentencing guidelines which enable prosecutors to cheat citizens of their constitutionally guaranteed right to a fair trial, by a jury of their peers — the federal sentencing guidelines which are in

3. Information theft: Information theft involves "hacking into a private network and stealing information" or data.[33] Publication or release of the stolen data sometimes follows the attack.[34] For example, in response to HBGary Federal CEO Aaron Bar's announcement that he planned to unmask the identity of various Anonymous members, Anonymous hacked HBGary's servers and published over 40,000 company emails.[35]

4. Virtual sabotage: Virtual sabotage involves "online activities designed to manipulate or damage the information technologies of the target. This includes the creation of viruses or worms: self-executing software programs that propagate and distribute messages or sabotage."[36] For example, one of the first-recorded acts of hacktivism involved dissemination of the anti-nuclear "WANK" worm, which penetrated computers at NASA and the U.S. Energy Department and altered log-in screens to read "WORMS AGAINST NUCLEAR KILLERS . . . Your System Has Been Officially WANKed."[37]

2. How Hacktivism Compares with Traditional Protests

When considering hacktivism in terms of the questions who, when, where, why, and how, hacktivism exhibits characteristics of traditional protests in the why, when, and where categories. First, hacktivists claim similar motivations — to effect political or social change, often in response to a particular political or social event — to those of traditional protestors.[38] Second, hacktivists, like most protestors, are motivated to execute cyberattacks during times likely to at-

---

clear violation of the 8th amendment protection against cruel and unusual punishments.

Id.

33. Samuel, *supra* note 19, at 11.

34. *Id.*

35. Andy Greenberg, *HBGary Execs Run for Cover as Hacking Scandal Escalates*, FORBES (Feb. 15, 2011, 8:55AM), http://www.forbes.com/sites/andygreenberg/2011/02/15/hbgary-execs-run-for-cover-as-hacking-scandal-escalates. The hack itself was embarrassing enough for HBGary as a security company; the emails also revealed "a long list of borderline illegal tactics" employed by the company. *Id.*

36. Samuel, *supra* note 19, at 11.

37. McCormick, *supra* note 6. The attack is said to have been in protest of the launch of a plutonium-fueled Galileo probe. Corinne Iozzio, *The 10 Most Mysterious Cyber Crimes*, PC MAG. (Sept. 26, 2008), http://www.pcmag.com/article2/0,2817,2331225,00.asp.

38. *See, e.g.*, *supra* notes 7–10 and accompanying text. Some critics may be quick to point out that some hacktivist participants are simply in it "for the lulz." *Cf.* Taylor Armerding, *Hacktivism Gets Attention, But Not Much Long-Term Change*, CSO ONLINE (Nov. 29, 2012), http://www.csoonline.com/article/722694/hacktivism-gets-attention-but-not-much-long-term-change ("Another thing that tends to undermine general public support for hacktivists is that they frequently acknowledge that their exploits are 'for the lulz' . . . ."). However, to argue that hacktivism is motivated by having fun at the expense of others is to discredit the significance of and motivation behind cyberattacks such as Operation Payback and Operation Last Resort.

tract the most attention.[39] Third, cyberattacks exhibit similarities to sit-in and picketing protests in that they often exploit attention directed at the target's property to gain publicity from a relevant audience.[40]

Hacktivism differs from traditional protests in the remaining who and how categories, specifically who participates and how it is conducted. First, cyberattacks can dupe the computers of others into involuntary participation in the attack.[41] Thus, the voluntariness of participation in a cyberattack can vary. In addition, hacktivism generally requires a certain level of technical know-how, but hacktivists have developed ways to enable layperson participation.[42] Furthermore, when compared with traditional protests, cyberattacks are less costly to execute in terms of actual resources[43] as well as physical effort and public presence.[44] This cuts in two separate ways: (1) technology lowers the barriers to participation,[45] and (2) fewer active participants are required to execute an effective cyberattack (as compared with a traditional protest).[46] Second, while traditional protests are accomplished through picketing, marches, or public sit-ins, hacktivism is accomplished through a variety of digital tools, often from behind a computer screen. Although traditional protests may be disruptive to the target's business by making it inconvenient or difficult for patrons or visitors to access the target's physical property, successful cyberattacks can often be more disruptive because they can more readily prevent digital access, even if just for a finite period of time.

---

39. *See, e.g.*, BARRACUDA NETWORKS, THE BARRACUDA WEB APPLICATION FIREWALL: BEST PRACTICES FOR PLANNING AND DEFENDING AGAINST ATTACKS BY ANONYMOUS, *available at* https://www.barracuda.com/assets/docs/White_Papers/Barracuda_Web_Application_Firewall_WP_Defending_Against_Anonymous.pdf (last visited Dec. 20, 2013) ("Often, [a DDoS] attack happens during peak traffic to gain additional visibility and leverage.").

40. *See infra* Section IV.A.2.

41. *See supra* note 25 and accompanying text.

42. *See supra* note 26 and accompanying text.

43. *See, e.g.*, Jeremy Kirk, *U.S. Power Companies Under Frequent Cyberattack*, PC WORLD (May 21, 2013, 6:45 PM), http://www.pcworld.com/article/2039480/us-power-companies-under-frequent-cyberattack.html; Mathew J. Schwartz, *10 Strategies to Fight Anonymous DDoS Attacks*, INFO. WEEK (Feb. 8, 2012, 8:00 AM), http://www.informationweek.com/security/vulnerabilities/10-strategies-to-fight-anonymous-ddos-at/232600411 (noting that "DDoS attacks are cheap to launch").

44. *See* McLaurin, *supra* note 15, at 245–46 ("Hidden behind individual computer screens, even well-meaning dissidents . . . are at best participating in a shallow gesture. The relative or actual anonymity that participants enjoy in large-scale DoS attacks depersonalizes their message, requires much less commitment, and thus evidences much less conviction than a public act of disobedience . . . ." (footnotes omitted)).

45. *See, e.g.*, Johnson, *supra* note 26.

46. *See, e.g.*, *supra* note 25 and accompanying text (describing the use of botnets to expand participation).

B. Criminal Liability Under the Computer Fraud and Abuse Act

There are at least forty different federal statutes that apply to computer-related crimes.[47] Each state has also enacted computer crime statutes to address computer misuse.[48] Analyzing all of these possible grounds for finding criminal liability for hacktivists is beyond the scope of this Note. Rather, this Note focuses on the federal statute most applicable to our discussion on criminal liability for hacktivism — the CFAA.[49]

The CFAA's primary provisions prohibit knowingly or intentionally (1) accessing exclusive government computers or classified information without authorization,[50] (2) obtaining information from computers through unauthorized access,[51] (3) committing fraud through unauthorized access,[52] (4) threatening to engage in cybercrime as a means of extortion,[53] and (5) generally taking actions that cause damage to protected computers.[54] This last provision, § 1030(a)(5), is the most relevant to the present discussion on hacktivism.[55]

Given the CFAA's broad definition of "protected computer,"[56] § 1030(a)(5) essentially "criminalizes intentionally or recklessly damaging virtually any computer connected to the Internet."[57] Even

---

47. Hampson, *supra* note 24, at 525.

48. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615 (2003).

49. 18 U.S.C. § 1030 (2012).

50. *Id.* at § 1030(a)(1), (3).

51. *Id.* at § 1030(a)(2).

52. *Id.* at § 1030(a)(4), (6).

53. *Id.* at § 1030(a)(7).

54. *See id.* § 1030(a)(5).

55. This provision criminalizes activity that:

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Id. Section 1030(a)(2) likely also applies to hacktivism, especially to cyberattacks that result in information theft. *See id.* § 1030(a)(2); *supra* note 33.

56. § 1030(e)(2) (defining a "protected computer" as a computer either (1) "exclusively for the use of a financial institution or the United States government," or (2) "used in or affecting interstate or foreign commerce or communication . . . of the United States").

57. Kesan & Hayes, *supra* note 3, at 493; *accord* Hampson, *supra* note 24, at 525; McLaurin, *supra* note 15, at 228 ("[The CFAA's] prohibitions cover practically any instance of cybercrime nationally because of the statute's expansive definition of 'protected computers.'"). This has led to much criticism of the CFAA's broad and vague language. *See, e.g.*, Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html. Stewart Baker has observed that:

though cyberattacks do not *physically* harm the target's computer or network elements, the CFAA's broad definitions of "damage"[58] and "loss"[59] likely bring cyberattacks within the scope of the CFAA's prohibitions.[60] For example, DDoS attacks and website redirects impair the availability of the targeted website.[61] Website defacements impair the integrity of data on the targeted website.[62] Information theft requires impairing the integrity of the targeted system to allow the hacktivist to gain access to the confidential information.[63] And virtual sabotage, by definition, impairs the information technologies of the targeted system.[64] Most of the negative effects felt by the target as a result of a cyberattack therefore fall within the CFAA's broad definition of causing loss to the target.[65]

III. FIRST AMENDMENT PROTECTION FOR HACKTIVISM

A. Three Rationales for the Protection of Speech

Courts and scholars alike generally agree that First Amendment jurisprudence is built upon "a patchwork of different interests underlying the protection of speech."[66] Three rationales for the protection of speech feature prominently in the literature: (1) the pursuit of truth,

---

> [T]he remarkable growth in cyberattacks . . . has enabled [the Justice Department] to turn the CFAA into what may be the most prosecutor-friendly criminal statute . . . . [A]ny competent prosecutor can find a way to indict and convict anyone who does anything Really Bad with a computer.

Stewart Baker, *Poisoning the Hamburger Helper*, VOLOKH CONSPIRACY (Sept. 11, 2011, 4:49 PM), http://www.volokh.com/2011/09/11/poisoning-the-hamburger-helper.

58. *See* § 1030(e)(8) (defining "damage" as "any impairment to the integrity or availability of data, a program, a system, or information").

59. *See id.* at § 1030(e)(11) (defining "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service").

60. *See* McLaurin, *supra* note 15, at 229 ("Based on this definition [of 'damage'], it is clear that liability under the CFAA should attach to any perpetrator of a DoS attack who intends the effects that an attack has on a server and has not been authorized to carry out the attack by the server's owner.").

61. *See supra* notes 22–26, 29, and accompanying text.

62. *See supra* note 31 and accompanying text.

63. *See supra* notes 33–35 and accompanying text.

64. *See supra* note 36 and accompanying text.

65. For example, the target could easily argue that the forms of impairment mentioned above resulted in *some* reasonable cost to it, whether in the form of lost business from a downed website or conducting a damage assessment to determine how to recover from the attack.

66. David S. Han, *Autobiographical Lies and the First Amendment's Protection of Self-Defining Speech*, 87 N.Y.U. L. REV. 70, 89 (2012) (footnote omitted).

(2) the promotion of democratic self-governance, and (3) the preservation of self-fulfillment and autonomy.[67]

The pursuit of truth rationale, commonly associated with John Stuart Mill, is rooted in the idea that the best test for truth is a robust "marketplace of ideas," where truth emerges from competition between conflicting ideas and opinions.[68] The promotion of democratic self-governance rationale, most closely associated with Alexander Meiklejohn, posits that effective self-governance necessarily requires the free exchange of ideas to inform the citizenry's decision-making.[69] Finally, the preservation of self-fulfillment and autonomy rationale, of which there are several different versions,[70] emphasizes the essential role that freedom of expression plays in developing individual personhood.[71]

It is important to note that, under the pursuit of truth rationale, suppression of even purportedly false or misleading speech is disfavored.[72] Rather, the ability to test false or misleading speech is considered an essential element of the discovery of truth — the eventual rejection of such speech creates "the clearer perception and livelier impression of truth."[73] The self-governance rationale, on the other hand, suggests that neutral government regulation of the "marketplace" of ideas is preferred and permissible, as long as it promotes a well-functioning democratic regime.[74] Under this view, the First Amendment is primarily concerned with the protection of public discourse and speech that promotes the public's ability to "propose, debate, and share ideas and information in order to rule effectively."[75]

---

67. GEOFFREY R. STONE ET AL., THE FIRST AMENDMENT 9–14 (Vicki Been et al. eds., 4th ed. 2012); Han, *supra* note 66, at 89–93. See STONE ET AL., *supra*, at 14–15, for a discussion of four additional theories that the First Amendment furthers interests in (1) checking the abuse of power by the government, (2) channeling conflict through expression rather than force, (3) promoting a tolerant society, and (4) development of valuable character traits in individual members.

68. Han, *supra* note 66, at 90 (discussing Justice Holmes' formulation of the "marketplace of ideas" metaphor in his famous dissent in *Abrams v. United States*, 250 U.S. 616, 630 (1919)).

69. *Id.* at 90–91.

70. *See* STONE ET AL., *supra* note 67, at 13.

71. *See* Han, *supra* note 66, at 92–93 (discussing how free speech helps develop our individual capacities to deliberate, reach conclusions, and act on those conclusions as free and rational persons).

72. *See id.* at 90.

73. *Id.* at 90 (quoting JOHN STUART MILL, ON LIBERTY 87 (David Bromwich & George Kate eds., Yale Univ. Press 2003) (1959)).

74. *See* Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757, 1762 (1994–1995).

75. Han, *supra* note 66, at 91. As Professor Sunstein argues persuasively, the self-governance rationale is superior to the pursuit of truth rationale given its consistency with history and the "highest ideals of American constitutionalism." Sunstein, *supra* note 74, at 1762–63.

B. Primary Obstacle To Extending First Amendment Protection to Hacktivism

1. The Public Forum Doctrine

The primary obstacle to invoking constitutional protection for hacktivism as free speech rests with the inherent limitations on the First Amendment's coverage. The First Amendment only affords constitutional protection against a specific *actor* — the government[76] — abridging free speech asserted in a specific *context* — the "public forum."[77] Although prosecution under the CFAA certainly meets the state action requirement, the unique nature of cyberspace — specifically, the high degree of public accessibility of most webpages — makes the question of whether privately owned or government-owned websites constitute public forums in cyberspace less straightforward.

a. Access to Private Property

To the extent that a privately owned website is considered private property, the law is well-settled that the First Amendment generally does not protect speech on private property against the wishes of the owner.[78] After the Supreme Court's decision in *Hudgens v. NLRB*, the sole surviving exception to this general rule is *Marsh v. Alabama*, which contains favorably broad language suggesting that public accessibility to private property can transform the character of the property from private to public for purposes of the First Amendment.[79] However, given *Hudgens*' narrow framing of *Marsh* as an exception involving a "company town" that "perform[ed] the full spectrum of

---

76. Under the "state action" doctrine, the First Amendment only guarantees constitutional protection against abridgment by the federal or state government. *See* MELVILLE B. NIMMER, NIMMER ON FREEDOM OF SPEECH § 4.01[A–B] (1984). Thus, the First Amendment affords no remedy against a private corporation or person who seeks to abridge the free expression of others. *See, e.g.*, Hudgens v. NLRB, 424 U.S. 507, 513 (1976). However, the state can become involved, and hence give rise to state action, when a private corporation or person involves the government in suppressing the speech of others, commonly in the form of asserting private property rights to exclude the speech. *See* NIMMER, *supra*, § 4.09[D].

77. *See* NIMMER, *supra* note 76, § 4.09[D] ("In the modern era the Supreme Court has . . . creat[ed] an abstraction known as the 'public forum.' The underlying premise is that freedom of speech under the First Amendment extends to, but only to, those sites which constitute 'public forums.'").

78. *See e.g.*, *Hudgens*, 424 U.S. 507; Lloyd Corp. v. Tanner, 407 U.S. 551 (1972).

79. *See* Marsh v. Alabama, 326 U.S. 501, 506–09 (1946) ("The more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it."). *But see Lloyd*, 407 U.S. at 569 ("Nor does property lose its private character merely because the public is generally invited to use it for designated purposes. Few would argue that a free-standing store, with abutting parking space for customers, assumes significant public attributes merely because the public is invited to shop there.").

municipal powers and stood in the shoes of the State," this exception for a private owner is unlikely to arise in most instances and therefore will not be discussed at length in this Note.[80]

b. Access to Government-Owned Property

Even with government-owned property, the First Amendment's protections are not guaranteed simply when speech occurs on such property.[81] The government, "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."[82] The Supreme Court has adopted the public forum doctrine for "determining when the Government's interest in limiting the use of its property . . . outweighs the interest of those wishing to use the property for [speech] purposes."[83] The public forum doctrine turns on the nature of the forum[84] and whether it falls into one of three categories of government-owned property: (1) traditional public forums, (2) designated public forums, and (3) nonpublic forums.[85]

Traditional public forums, such as public streets or parks, are defined by tradition and history as forums that have "immemorially been held in trust for the use of the public and . . . used for purposes of assembly, communicating thoughts between citizens, and discussing public questions."[86] In addition to traditional public forums, the gov-

80. *Hudgens*, 424 U.S. at 519; *see also* NIMMER, *supra* note 76, § 4.09[D] ("[I]t seems clear that the 'full spectrum of municipal powers' standard invoked in *Lloyd* and ratified in *Hudgens* vitiates First Amendment access claims not only in privately owned shopping centers, but in many other privately owned premises otherwise open to the public."). The First Amendment and shopping center saga, however, did not end at *Hudgens*. In *PruneYard Shopping Center v. Robins*, the Supreme Court held that a state can choose to strike the balance differently — a state Constitution's free speech guarantee may override private property interests by allowing the public to seek First Amendment protection for engaging in speech activities at a privately owned shopping center. *See* 447 U.S. 74, 81 (1980) (discussing a state's "sovereign right to adopt in its own Constitution individual liberties more expansive than those conferred by the Federal Constitution" and that the state "in the exercise of its police power may adopt reasonable restrictions on private property so long as the restrictions do not amount to a taking without just compensation or contravene any other federal constitutional provision"). The Court held the state constitution's protection of free speech did not amount to a taking of the private property because the owners "failed to demonstrate that the 'right to exclude others' is so essential to the use or economic value of their property that the state-authorized limitation of it amounted to a 'taking.'" *Id.* at 84. At the very least, *PruneYard* makes clear that speech activities conducted on private property may nevertheless be protected to a certain extent by a state's constitution, even if not by the First Amendment. *See id.* at 88.

81. *See* Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 46 (1983).

82. Greer v. Spock, 424 U.S. 828, 836 (1976) (quoting Adderley v. Florida, 385 U.S. 39, 48 (1966)).

83. Cornelius v. NAACP Legal Def. & Educ. Fund, Inc., 473 U.S. 788, 800 (1985).

84. *See id.*

85. David J. Goldstone, *A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech*, 69 U. COLO. L. REV. 1, 8 (1998).

86. *Perry*, 460 U.S. at 45 (quoting Hague v. CIO, 307 U.S. 496, 515 (1939)).

ernment may also create designated public forums if the property itself has not "traditionally been regarded as a public forum [and] is intentionally opened up for that purpose."[87] Speech asserted in both traditional and designated public forums receives the highest degree of First Amendment protection. This means that content-neutral restrictions are subject to a test of reason, and content-based restrictions are subject to strict scrutiny.[88] All other forms of government-owned property are nonpublic forums. The government can restrict access to speech in nonpublic forums so long as the restrictions are reasonable and viewpoint-neutral.[89]

c. Websites in Cyberspace — Private, Public, or Nonpublic Forum?

i. Privately Owned, Public-Facing Websites

Can public-facing websites[90] created by private individuals or companies be considered public forums? No reported case has explicitly reached the issue of whether privately created websites are public forums for First Amendment purposes, but developments in case law applying the doctrine of trespass to alleged violations of a website's terms of use support the notion that websites created by private individuals or companies constitute private property.[91] Additionally, two federal district courts have declined to find that a private company's *email system* constitutes a public forum.[92] Although the degree of public accessibility is significantly higher for a public-facing website than for an email system, such cases at least suggest that privately

87. Pleasant Grove City v. Summum, 555 U.S. 460, 469 (2009)

88. *See id.* at 469–70.

89. Ark. Educ. Television Comm'n v. Forbes, 523 U.S. 666, 676 (1998); Cornelius v. NAACP Legal Def. & Educ. Fund, Inc., 473 U.S. 788, 800 (1985).

90. Public-facing websites are those that are generally available to the public.

91. *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 482–83, 505 (2003) ("The trespass to chattels and computer trespass actions, applied to cyberspace [by courts], operate using precisely this framework. You are forbidden from entering a cyberspace place except upon conditions set by the space's proprietor."); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 527 n.24 (2003) (listing representative cases applying the law of trespass to cyberspace in the form of email and websites).

92. *See* Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 446 (E.D. Pa. 1996) ("AOL's e-mail servers are certainly not a traditional public forum . . . . Instead, AOL's e-mail servers are privately owned and are only available to the subscribers . . . . Moreover . . . AOL has not presented its e-mail servers to the public at large for disseminating political messages at a certain event."); s*ee also* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1025 (S.D. Ohio 1997) (holding that there is no First Amendment right to send unobstructed emails to AOL subscribers when AOL "was not exercising powers that are traditionally the exclusive prerogative of the state, such as where a private company exercises municipal powers by running a company town"). Although both courts highlighted the commercial nature of the speech, the significance of this fact and how it interacts with the public forum doctrine is unclear. *See* Goldstone, *supra* note 85, at 12, 14–17.

managed forms of electronic communication constitute private forums.

Thus, under current doctrine, cyberattacks against privately created websites are unlikely to qualify for constitutional protection under the First Amendment. The classification of such websites as private property precludes application of the public forum doctrine. As a result, only private owners of websites who meet the extraordinarily high standard articulated in *Hudgens*[93] may be required to permit access to the private property for speech activities under the First Amendment.

ii. Public-Facing Government Websites

Can public-facing websites created by the government be considered public forums? Four federal circuits[94] and the California Supreme Court[95] have expressly rejected this notion. These cases arose in disputes over whether the government had violated the First Amendment by refusing requests to post hyperlinks or other content to government-owned websites.[96] The First and Fourth Circuits found that town websites constituted government speech,[97] which is not sub-

93. *See supra* note 80 and accompanying text.

94. *See* Sutliffe v. Epping Sch. Dist., 584 F.3d 314, 333–34 (1st Cir. 2009) (questioning the application of the public forum doctrine to a town's website and concluding that the website was neither a traditional nor a designated public forum); Hogan v. Twp. of Haddon, 278 F. App'x 98, 102 (3d Cir. 2008) (stating that a website is "local government-owned and sponsored," and is therefore not a "public or limited public forum[]. Thus, Hogan had no constitutional right to . . . post on the Township's website . . . ."); Page v. Lexington Cnty. Sch. Dist. One, 531 F.3d 275, 285 (4th Cir. 2008) ("[W]e conclude that the School District sufficiently controlled [its own website] so that its speech remained government speech and it did not create a limited public forum by including links to other websites."); Putnam Pit v. City of Cookville, 221 F.3d 834, 844–45 (6th Cir. 2000) (holding that a municipal website is a nonpublic forum, which can be subject to viewpoint-neutral restrictions). Although unrelated to government-owned websites, the *Perry* case held that a public school's email system was a nonpublic forum because it was neither a traditional public forum nor had the school opened the system to indiscriminate use by the general public to constitute a designated public forum. Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45–47 (1983).

95. *See* Vargas v. City of Salinas, 205 P.3d 207, 215 n.8 (Cal. 2009) (affirming the court of appeals' rejection of plaintiff's argument that the city's website constituted a public forum because the "[c]ity had not permitted private individuals or groups to post material on its Web site or to publish articles in its newsletter").

96. *See, e.g.*, *Sutliffe*, 584 F.3d 314 (request by citizen group to add a hyperlink on the town's website when the town permitted other organizations to post hyperlinks); *Hogan*, 278 F. App'x 98 (request to post articles written by the township Commissioner on township's website); *Page*, 531 F.3d 275 (request for equal access to school district's website to present the opposing viewpoint on a bill); *Putnam Pit*, 221 F.3d 834 (request by tabloid focused on city corruption to add a hyperlink to the tabloid's webpage on the city website); *Vargas*, 205 P.3d 207 (request by proponents of local ballot initiative to post information supporting the ballot initiative to the city's website).

97. *See Sutliffe*, 584 F.3d at 329; *Page*, 531 F.3d at 285. In dicta, the First and Fourth Circuits did acknowledge that the government's lack of control over private content and its lack of discretion in removal of private content could transform the website into a designat-

ject to First Amendment analysis.[98] The Third and Sixth Circuits, as well as the California Supreme Court, have similarly concluded that such websites are nonpublic forums because they are neither immemorially held as traditional public forums nor opened up to the public generally as public forums.[99]

Aside from these applications of doctrinal legal categories, the courts have also voiced prudential concerns over equating a public-facing government website with a designated public forum. For example, the First Circuit opined that the public forum doctrine "could risk flooding the Town website with private links, thus making it impossible for the Town to effectively convey its own message."[100] The court reasoned that a government entity "[f]aced with a rule that would force it to open its website to private speech to such a degree that it is unable to communicate its own message . . . might reasonably choose to simply eliminate all external links from its website," which would perversely "lead to less, not more, speech."[101]

Although the Supreme Court has yet to reach the issue of whether government websites qualify as public forums, under the current development of case law, a static government-owned website intended only to convey information will likely be deemed either government speech or a nonpublic forum. Under either scenario, no First Amendment protection would extend to private speech expressed on such websites — in the form of cyberattacks or otherwise.[102] Thus, inherent

---

ed public forum. *Sutliffe*, 584 F.3d at 334–35 ("It is possible there may be cases in which a government entity might open its website to private speech in such a way that its decisions on which links to allow on its website would be more aptly analyzed as government regulation of private speech."); *Page*, 531 F.3d at 283–85.

98. Pleasant Grove City v. Summum, 555 U.S. 460, 467 (2009) ("The Free Speech Clause restricts government regulation of private speech; it does not regulate government speech.").

99. *Putnam Pit*, 221 F.3d at 843 ("Even if public fora are not limited by their historic confines, these places still must, by definition, be 'open for expressive activity regardless of the government's intent.' . . . The municipal Web site . . . do[es] not allow for open communication or the free exchange of ideas between members of the public." (citations omitted)); *Hogan*, 278 F. App'x at 102; *Vargas*, 205 P.3d at 230 n.18.

100. *Sutliffe*, 584 F.3d at 334.

101. *Id.* at 334. The court in Illinois Dunesland Preservation Society v. Illinois Department of Natural Resources expressed a similar view in writing the following:

> [M]ust the park on request link its online home page to every website of an organization or a person who would like to express an opinion on asbestos fibers or any other topic that might relate to Illinois Beach State Park? We can guess what the effect of the position urged by the plaintiff in this case would be: . . . no more home pages for public agencies. We can avoid that end by avoiding this beginning.

Ill. Dunesland Pres. Soc'y v. Ill. Dept. of Natural Res., 584 F.3d 719, 725–26 (7th Cir. 2009) (citations omitted).

102. The government today, however, operates thousands of websites. While many are strictly informational and lack opportunities to engage the public, a growing number of government websites have leveraged interactive social media tools to "solicit public input and foster public discussion." David S. Ardia, *Government Speech and Online Forums: First Amendment Limitations on Moderating Public Discourse on Government Websites*,

limitations on the First Amendment's coverage, encompassed by the public forum doctrine, present a primary obstacle to invoking constitutional protection for hacktivism as free speech.

C. Secondary Arguments Against Extending First Amendment Protection to Hacktivism

1. "Internet Exceptionalism"

"Internet exceptionalism" is predicated on the notion that the Internet is a "unique and wholly new medium" requiring Internet-specific rules that diverge from the existing legal system.[103] Some commentators argue that compared to traditional protests, cyberattacks are easier to execute and enable participants to hide behind their computer screens, thus rendering them a less-valued form of protest.[104] However, line-drawing between forms of protest that do or do not merit First Amendment protection should not be based on the notion that technological innovation somehow transforms the nature of an activity. Penalizing the efficient evolution of communications arising from new technology — by casting cyberattacks in a different category *solely* on the grounds that the ease of launching a cyberattack fundamentally changes the nature of the activity — would run counter to First Amendment purposes.[105] After all, the use of technology that

---

2010 BYU L. REV. 1981, 1986–87 (2010). In light of this change, the courts will likely entertain more arguments that such websites constitute limited public forums. *Id.* at 2026. In the case of cyberattacks against such interactive government websites, the courts may come to recognize these sites as limited public forums that do not present obstacles to First Amendment protection. The interactivity of websites, however, may act as a double-edged sword that weighs against the need for cyberattacks to receive free speech protection, given ample alternatives under the content-neutral restrictions doctrine. *See infra* Section IV.D.

103. Eric Goldman, *The Third Wave of Internet Exceptionalism*, TECH. & MARKETING LAW BLOG (Mar. 11, 2009), http://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm.

104. *See, e.g.*, McLaurin, *supra* note 15, at 245–46; *supra* text accompanying note 44; Adam Popescu, *DDoS Attacks as Social Protest*, READWRITE (Jan. 22, 2013), http://readwrite.com/2013/01/22/petition-to-legitimize-ddos-attacks-and-other-tomfoolery. Critics also argue that the anonymity of hacktivists undermines their potential First Amendment claims. *See supra* note 44. However, anonymity has never been a sufficient reason alone to strip a speaker of First Amendment protection. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."). Furthermore, "electronic *pseudonymity* — anonymity through the adoption of an alias — can have the parallel effect of constructing a kind of public voice even as it protects personal identity." DIANA SACO, CYBERING DEMOCRACY: PUBLIC SPACE AND THE INTERNET 119 (Univ. of Minn. Press, 2002).

105. *Cf.* Brown v. Entm't Merch. Ass'n, 131 S. Ct. 2729, 2738 (2011) (holding that even violent video games are entitled to First Amendment protection because the difference between video games and literature is "more a matter of degree than of kind").

makes it easier and less costly to contribute to public discourse should be encouraged as furthering First Amendment interests.[106]

It remains important to recognize, however, that technology can facilitate not only socially productive activities, but also socially destructive activities.[107] The aggregative and disaggregative properties of technology minimize the cost of both productive and destructive social behavior.[108] For example, in the context of cyberattacks, technology aggregates by facilitating organization and collaboration among people of distant geographies; technology also disaggregates by allowing people to separate their voice from their physical presence.[109] "The challenge for law is to foster positive applications of technology's potential while understanding and checking as many of its destructive applications as possible."[110]

As the Supreme Court has announced: "whatever the challenges of applying the Constitution to ever-advancing technology, 'the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary' when a new and different medium for communication appears."[111] It is therefore important to apply legal doctrines with a nuanced understanding of what the technology does rather than how it works.[112] The Internet exceptionalism mentality is flawed, and the use of technology to create new mediums for communication should not warrant narrower application of First Amendment principles.

---

106. *Cf.* Martin v. City of Struthers, 319 U.S. 141, 146 (1943) (upholding the right to distribute leaflets door-to-door because it was "essential to the poorly financed causes of little people").

107. *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 63 (2009).

108. *See id.*

109. *Id.*

110. *Id.*

111. Brown v. Entm't Merch. Ass'n, 131 S. Ct. 2729, 2733 (2011) (quoting Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 503 (1952)).

112. As Professor Kerr has remarked:

> Like museumgoers eyeing a Seurat painting from inches away, judges and legislators have viewed Internet code and communications as 0's and 1's zipping around the world, without much consideration of what the 0's and 1's are there to do. This failure to appreciate code as a backdrop to the virtual world of cyberspace has led courts to embrace an Internet formalism characterized by broad rules that apply equally to all code regardless of its contents. In short, Internet law tends to regulate code based on what the code *is*, rather than the more nuanced conception of what the code *does*.

Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287, 1288 (2000).

2. The Speech/Conduct Dichotomy

Another likely objection to invoking constitutional protection for hacktivism lies in the speech/conduct dichotomy. While free speech protects more than merely verbal communications of ideas,[113] conduct does not receive such expansive protection "whenever the person engaging in the conduct intends thereby to express an idea."[114] However, prior extension of the First Amendment to "the peaceful expression of views by marchers, demonstrations or assemblies"[115] demonstrates how certain conduct may be "sufficiently imbued with elements of communication to fall within the scope" of the First Amendment.[116]

The courts make a distinction between "'pure speech' which is entitled to the full panoply of First Amendment protection, and symbolic speech or speech plus, which is to receive some ill-defined lesser degree of protection."[117] In deciding whether particular conduct possesses sufficient communicative elements to qualify as symbolic speech and bring the First Amendment into play, the courts ask whether intent to convey a particularized message was present and whether the likelihood was great that the message would be understood by those who viewed it.[118]

Are cyberattacks "speech" within the meaning of the First Amendment? Cyberattacks are not verbal expressions, although they may employ verbal expressions based in text or media. The attack itself is more properly analyzed as conduct, so the better question becomes whether cyberattacks qualify as symbolic speech so as to bring the First Amendment into play.[119]

---

113. NIMMER, *supra* note 76, § 3.06.

114. United States v. O'Brien, 391 U.S. 367, 376 (1968).

115. *See* Davis v. Francois, 395 F.2d 730, 733 (5th Cir. 1968).

116. Texas v. Johnson, 491 U.S. 397, 404 (1989) (quoting Spence v. Washington, 418 U.S. 405, 409 (1974)).

117. NIMMER, *supra* note 76, § 3.06[B] (footnote omitted).

118. *Id.* Even though the Court has found that nonverbal conduct such as the burning of a flag or the wearing of a black armband to protest the Vietnam War constitutes symbolic speech within the protection of the First Amendment, the Court has also questioned the expressiveness of burning a draft card in protest of the Vietnam War. *Compare Johnson,* 491 U.S. 397, *and* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969), *with O'Brien*, 391 U.S. at 376 ("[E]ven on the assumption that the alleged communicative element in O'Brien's conduct is sufficient to bring into play the First Amendment, it does not necessarily follow that the destruction of a registration certificate is constitutionally protected activity.").

119. Even though some federal appellate courts have recognized computer code as expressive conduct protected by the First Amendment, the rationale for protection is unlikely to extend to cyberattacks, even though the attacks themselves also rely on code. The courts in these cases emphasized the use of computer code as an "expressive means for the exchange of information and ideas about *computer programming*." Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) (emphasis added); *see also* Universal City Studios v. Corley, 273 F.3d 429 (2001). One could not sincerely argue that the purpose of hacktivism is to exchange information about computer programming. Thus, we turn to examine whether

To begin, it is unlikely that information theft or virtual sabotage qualify as symbolic speech. Both are conducted in stealth, which undermines any argument of an intended audience. Furthermore, critics argue that DDoS attacks are mere conduct, devoid of expression because a downed website does not communicate the content of any intended message.[120] Although the hacktivists may intend to communicate their disapproval of the target by taking down the website, the meaning behind a DDoS attack would likely not be apparent to visitors for whom the website simply fails to load.[121] Although most forms of cyberattacks are unlikely to qualify as symbolic speech, website redirects and website defacements may qualify depending on the content displayed as a part of the redirect or defacement.

3. The Censorial Nature of Cyberattacks

Another common objection to First Amendment protection for cyberattacks relates to the perception that cyberattacks are censorial in nature: "You don't stand up for free speech by using a muzzle."[122] Certain forms of speech, such as hate speech, have long been subject to limitations consistent with the First Amendment partly on the premise that such speech may have a "silencing" effect on public discourse and its prohibition will have a positive net effect on public discourse.[123]

---

cyberattacks merit First Amendment protection outside the context of computer coding as expressive conduct.

120. *See* McLaurin, *supra* note 15, at 235.

121. *See id*. However, the Supreme Court has emphasized that in determining whether conduct qualifies as symbolic speech, the Court considers the context in which the conduct occurred. *See Johnson,* 491 U.S. at 405. To the extent news reporting and media coverage regarding the DDoS attacks factor into the context in which the conduct occurred, it is arguable that the intended message will be communicated, albeit through alternative sources.

122. Tom Watson, *Denial of Service, Denial of Speech [Updated]*, TOM WATSON — MY DIRTY LIFE & TIMES (Dec. 12, 2010), http://tomwatson.typepad.com/tom_watson/2010/12/denial-of-service-denial-of-speech.html.

123. As one scholar writes:

> [T]he state may have to act to further the robustness of public debate in circumstances where powers outside the state are stifling speech. It may have to allocate public resources — hand out megaphones — to those whose voices would not otherwise be heard in the public square. It may even have to silence the voices of some in order to hear the voices of the others.

OWEN M. FISS, THE IRONY OF FREE SPEECH, 3–4 (1996), *available at* http://www.washingtonpost.com/wp-srv/style/longterm/books/chap1/ironyoffreespeech.htm; *see also* Melissa Weberman, *University Hate Speech Policies and the Captive Audience Doctrine*, 36 OHIO N.U. L. REV. 553, 556–57 (2010) ("Hate speech is inconsistent with the marketplace of ideas because it 'inflects, skews, and disables the operation of the market[.]' It decreases the total amount of speech in the marketplace by its silencing effect on its target groups."). However, the Supreme Court has also recently rejected a related speech maximization theory in *Arizona Free Enterprise Club's Freedom PAC v. Bennett*. *See* 131 S. Ct. 2806, 2825 (2011) ("We have repeatedly rejected the argument that the government has a

Similarly, to the extent that a particular form of cyberattack has a net negative effect on public discourse or simply substitutes its speech for that of another, the First Amendment should not apply. Affording constitutional protection to such conduct would be inconsistent with the underlying rationales of the First Amendment in promoting the marketplace of ideas and maximizing public discourse for self-governance. Although under the self-fulfillment rationale, this exercise of speech may be said to further the hacktivist's self-autonomy, this rationale is limited to "foster[ing] individual self-realization and self-determination without improperly interfering with the legitimate claims of others."[124]

To the extent the information posted on a website constitutes speech by another party, most cyberattacks today are censorial in nature and therefore conflict with the notions of free speech under the First Amendment.[125] For example, DDoS attacks take down the targeted website, albeit temporarily. Similarly, a website redirect prevents a visitor from accessing the targeted website. And to the extent website defacement alters the original content on the targeted website, it also suppresses speech in the form of pre-existing content. Thus applying the rationales underlying the First Amendment, it is difficult to justify First Amendment protection for these particular forms of hacktivism, given their censorial nature.[126]

Setting aside these secondary concerns, however, the most compelling argument for rejecting a First Amendment defense for cyberattacks remains based on the inherent limitations to First Amendment coverage, as evidenced by the public forum doctrine discussed earlier in Section III.B. Current trends in First Amendment jurisprudence as applied to cyberspace demonstrate that the primary obstacle for such a

---

compelling state interest in 'leveling the playing field' that can justify undue burdens on political speech.").

124. Han, *supra* note 66, at 92 (quoting C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964, 966 (1978)).

125. *See* A.P. Karanasiou, *Occupying Cyberspace and Distributed-Denial-of-Service (DDoS) Attacks: The Changing Face of Protests in the Digital Age*, *in* POLITICS AND POLICY IN THE INFORMATION AGE (Jonathan Bishop & Ashu M. G. Solo eds., 2013) (forthcoming 2014).

126. This issue does present a line-drawing problem. The activities of Anonymous have had a chilling effect on its targets. *See, e.g.*, Alexander Abad-Santos, *How Anonymous Got Westboro to Back Off Aaron Swartz's Funeral*, ATLANTIC WIRE (Jan. 15, 2013), http://www.thewire.com/national/2013/01/anonymous-westboro-baptist-church-aaron-swartz-funeral/61036/ (discussing Westboro Baptist Church's decision to forgo plans to picket Aaron Swartz's funeral); Nate Anderson, *Anonymous vs. HBGary: The Aftermath*, ARS TECHNICA (Feb. 25, 2011), http://arstechnica.com/tech-policy/2011/02/anonymous-vs-hbgary-the-aftermath (discussing HBGary's withdrawal from a security conference). But as long as speech is deemed protected under the First Amendment, its chilling effects ex post are unlikely to strip First Amendment protection in the same way that truthful statements are protected by the First Amendment even if they are injurious to one's reputation. *See* RAYMOND T. NIMMER, 2 INFORMATION LAW § 10:9 ("Truth is a defense to a cause of action for defamation.").

defense will be the fact that a hacktivist has no First Amendment right to exercise speech "on" another's website.

IV. RECONCEPTUALIZING CYBERSPACE: "POP-UP SIDEWALKS" IN CYBERSPACE

"Minds are not changed in streets and parks as they once were."[127] The protection of free speech must take into account the new digital means of exchanging ideas and shaping the public consciousness. The First Amendment applies no less to forums that exist "more in a metaphysical than in a spatial or geographic sense."[128]

Yet the places where expression occurs in cyberspace are overwhelmingly privately owned, which, according to one critic, has led to the "death of the public forum in cyberspace."[129] This Section takes a critical look at the current direction of case law, particularly with respect to the privatization of cyberspace, and discusses an alternative conception of cyberspace where pop-up windows are analyzed under the First Amendment.

A. Two Central Premises to Hacktivism: The "Digital Attention Deficit" and the Need for "Specific Access"

1. Digital Attention Deficit — Finiteness of Attention

A central premise of hacktivism is the concept of "digital attention deficit," which is a limiting factor on the size of the audience that receives a protestor's message. Although millions of Americans can read a protestor's website, the question is how many in fact will do so, given the billions of other webpages competing for their tion.[130] As technology reduces the costs of disseminating and accessing content, the finiteness of audience attention becomes all the more apparent.[131]

---

127. Denver Area Educ. Telecomms. Consortium, Inc. v. FCC, 518 U.S. 727, 802–03 (1996) (Kennedy, J., concurring).

128. Rosenberger v. Rector & Visitors of Univ. of Va., 515 U.S. 819, 830 (1995); *see also* Reno v. ACLU, 521 U.S. 844, 870 (1997) ("We agree with [the] conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet].").

129. *See* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115 (2005).

130. *See* Kreimer, *supra* note 5, at 142–43 ("The reduction of the costs of access to a mass audience does not mean a similar reduction in the costs of actual communication with that audience, because the scarce resource in the emerging communications environment is limited audience attention.").

131. *Id.* at 143 ("As the cost of dissemination of information falls toward zero, the amount of available information increases toward infinity, and there are, after all, only twenty-four hours (and for most of us — sixteen waking hours) in the day.").

An attack on a target's website helps hacktivists maximize the audience receiving their message in the face of acute attention scarcity in cyberspace. Hacktivists leverage the target's website as a platform to promote their cause by effectively "stealing" the traffic and attention originally directed towards the target website.[132] This kind of "stolen attention" from the target website enables hacktivists to circumvent the digital attention deficit by garnering more attention than a separate website might otherwise attract on its own.

2. Specific Access

Another important premise of hacktivism is the concept of specific access. Public forums support two kinds of access to audiences: (1) "*general* access facilitated by forums through which people pass on their way to many destinations" and (2) "*specific* access facilitated by forums through which any person must pass if she is to enter a particular destination."[133] Specific access, in contrast to general access, is about the relevance of the audience members reached rather than the number of audience members reached.[134] For example, an aggrieved mother might rely on the public sidewalks adjacent to the skating rink where her son was injured to reach a specific audience — other patrons of the rink who might similarly be concerned about the safe operations of the business and have potential influence over the business' behavior.[135] "[S]ubstituting another place with a numerically equivalent audience would miss the point, because the audience the [mother] want[s] to reach is defined by its relationship to a specific place."[136] Yet the privatization of cyberspace hampers this notion of specific access because there is no online equivalent of a nearby public sidewalk.

Hacktivism circumvents the lack of specific access in cyberspace by forcibly creating specific access to a target website. This allows hacktivists "to avoid wasting resources on irrelevant audiences and to reach audience members in situations in which they are most likely to pay attention to the message and be able to act on it."[137]

---

132. *See id.* at 156. Groups bidding for digital audience attention can use a combination of three strategies: (1) beg for attention by seeking notice directly from a voluntary audience, (2) borrow the attention voluntarily provided by an audience of intermediaries, and/or (3) steal attention from another group's website by imposing their message directly on the other group's website to an involuntary audience. *Id.* at 144–56.

133. Noah D. Zatz, *Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment*, 12 HARV. J.L. & TECH. 149, 152.

134. *See id.* at 166, 170.

135. *See id.* at 225.

136. *Id.* at 166.

137. *Id.* at 167.

B. Pop-up Sidewalks as Public Forums

Cyberspace is no longer simply an extension of physical space.[138] Rather, cyberspace has become an *alternative* to physical space. In 2011, the average American spent at least 8.5 hours a day in front of a screen.[139] In the realm of e-commerce, consumers can choose to make purchases online without having to leave the comfort of their homes just as retailers can choose to launch online-only businesses without incurring the risks associated with opening a brick-and-mortar establishment.[140]

To the extent cyberspace has become an alternative to physical space, it is a unique forum for protest. Yet, there are no digital analogs to public sidewalks adjoining the physical presence of the target of protest in cyberspace.[141] For example, speakers who wish to protest against an online-only business would be hard-pressed to find a public forum that would provide them with specific access.

Some commentators argue that courts should adopt a more functional approach to the public forum doctrine in its application to cyberspace,[142] whereas others even contemplate treating privately owned websites as public forums.[143] Still others have explored the prospect of equating privately owned websites to places of public accommodation.[144]

Noah Zatz proposes that the solution to making room for public forums in cyberspace rests with conceptualizing pop-up windows as "cyber sidewalks."[145] After all, the public forum's value to the speaker is in both the degree to which the place is public, as well as the de-

---

138. *See id.* at 151 ("As [daily activities] increasingly shift from the physical environment of our cities and towns to the electronic environment of cyberspace, we must create 'the places in between,' that enable ordinary citizens to engage one another as they move between the places where they conduct their affairs.").

139. Pico Iyer, *The Joy of Quiet*, N.Y. TIMES (Dec. 29, 2011), http://www.nytimes.com/2012/01/01/opinion/sunday/the-joy-of-quiet.html?pagewanted=all.

140. *See Online Retailers Stealing Bricks and Mortar Business*, 24/7 WALL ST. (Dec. 1, 2011), http://247wallst.com/2011/12/01/online-retailers-stealing-store-customers.

141. *See generally* Zatz, *supra* note 133.

142. *See* Nunziato, *supra* note 129, at 1161–64.

143. *See, e.g.*, Ronnie Cohen & Janine S. Hiller, *Towards a Theory of Cyberplace: A Proposal for A New Legal Framework*, 10 RICH. J.L. & TECH. 2, para. 28 (2003), *available at* http://jolt.richmond.edu/index.php/623-2/volume-x-2003-2004/ (stating that a court may "classify a private web site as a public forum" because of its "interconnectedness with all other web sites" and due to "the history of the Internet as a government sponsored medium").

144. *Id.* at para. 41. Somewhat relatedly, although for anti-discrimination purposes, at least one federal court has held that private websites can be considered places of public accommodations and subject to regulation under the Americans with Disabilities Act. *See* Nat'l Ass'n of the Deaf v. Netflix, Inc., 869 F. Supp. 2d 169 (D. Mass. 2012).

145. *See* Zatz, *supra* note 133, at 210–11.

gree to which it facilitates access to the targeted property.[146] Without spatial proximity to the targeted website, other forums in cyberspace, such as personal websites, will be relatively useless because they fail to provide both general and, more importantly, specific access in the face of the digital attention deficit.[147]

Professor Lemley has criticized the conceptual leap that courts make in equating "place" with "property."[148] Instead, he argues that, if judges apply the "cyberspace as place" metaphor to cases involving cyberspace, judges should consciously determine whether this sort of "space" should be considered public space or private property.[149] Lemley argues that the balance should in fact tilt in favor of public space given that (1) the economic rationale underlying the privatization of land does not apply to cyberspace where information goods are nonrivalrous, and (2) the absence of physical proximity online renders privatized cyberspace unassailable in the sense that the public would have no recourse in adjacent access to the privatized "property" in cyberspace.[150] Finally, he asserts that, even if cyberspace can be privately owned, the "bundle of rights" associated with this particular property ownership in cyberspace could vary given the unique nature of cyberspace.[151] Thus, property interests in cyberspace could be "limited by easements or covenants . . . implied for [a] public purpose."[152]

---

146. *See id.* at 151 ("Paradigmatic public forums perform their function in our constitutional order not so much because of what happens *inside* them as because of what happens outside, or more precisely, *alongside* them.").

147. *See id.* at 192. To simulate spatial proximity to the targeted website, protestors in cyberspace currently rely on methods such as: (1) using the target's name or logo as one of the metatags for the protestor's critical website, (2) using the target's name as part of the domain name associated with the protestor's critical website, or (3) using the target's name or mark as a keyword in online advertisements criticizing the target. *See* Nunziato, *supra* note 129, at 1168. The first two methods, however, are unlikely effective in generating a specific audience unless a visitor is already specifically seeking out the critical website. The last method, while effective, is likely costly. *See, e.g.*, Darren Dahl, *Small Players Seek an Alternative to the Expense of Pay-Per-Click*, N.Y. TIMES (Oct. 17, 2012), http://www.nytimes.com/2012/10/18/business/smallbusiness/as-pay-per-click-ad-costs-rise-small-businesses-search-for-alternatives.html?_r=0.

148. *See* Lemley, *supra* note 91, at 532–33.

149. *See id.* at 536. *See generally* Hunter, *supra* note 91, at 443 ("[T]he received wisdom has confused the descriptive question of whether we think of cyberspace as a place with the normative question of whether we should regulate cyberspace as a regime independent of national laws.").

150. *See* Lemley, *supra* note 91, at 536–37; *see also* Zatz, *supra* note 133, at 222 ("Unlike one ejected from a strip mall parking lot, a speaker refused entry to a cyber-place cannot simply step over the property line and remain visible and audible to those entering or already within . . . one cannot simply relocate to the public sidewalks adjoining its pedestrian and automobile accessways.").

151. Lemley, *supra* note 91, at 537 (noting, as an example, the distinctions in the "bundle of sticks" associated with the rights we give to owners of real property as compared to owners of intellectual property).

152. *Id.* at 539. Professor Hunter has also explained how the privatization of cyberspace has pushed us to the brink of a digital anticommons. *See* Hunter, *supra* note 91, at 502 ("The anticommons effect occurs when multiple parties can prevent others from using a given resource so that no one has an effective right of use.").

The government has an "important affirmative role . . . in facilitating freedom of speech" in a world that is shifting increasingly to cyberspace.[153] The First Amendment may have to intervene in the allocation of property as well as the state's enforcement of private property interests[154] to correct imperfections in the market for free expression.[155] "[W]here private media fails to foster adequate public dialogue, the First Amendment requires the government to create at least some public forums that provide effective means of communication."[156] Just as the Supreme Court relied on the property law doctrine of easements to justify the public forum doctrine in removing plenary power from the government as property owner,[157] courts could similarly justify a pop-up window as an easement on a private or nonpublic website for the implied purpose of furthering public discourse.[158]

C. Cyberattacks that Generate Pop-ups

Building on and applying Zatz's suggestion to the context of hacktivism, a cyberattack that generates pop-up windows "adjacent" to the targeted website would, in effect, generate a cyber sidewalk (i.e., a public forum). The generation of the pop-up would then help such a cyberattack circumvent the obstacle that stands in the way of First Amendment protection for current forms of cyberattacks. Depending on whether or not the content of the pop-up constitutes symbolic speech, the cyberattack could qualify for First Amendment protection.

Although a pop-up that displays obscene materials is unlikely to qualify for First Amendment protection,[159] a pop-up window that displays a message with substantive criticism of the target likely meets the test for symbolic speech.[160] In the latter case, the intent to convey a symbolic message is readily discernible from the content, and the audience viewing the pop-up window is likely to understand that message, regardless of whether or not the audience sympathizes with it. Such an attack is qualitatively different from a DDoS attack because an informative pop-up window uses the attack as a *means* to deliver a message rather than relying on the mere existence of the attack to de-

153. Nunziato, *supra* note 129, at 1117.

154. *See* Zatz, *supra* note 133, at 172.

155. *See* Nunziato, *supra* note 129, at 1117.

156. Ardia, *supra* note 102, at 1999 (internal quotation marks omitted).

157. *See* Nunziato, *supra* note 129, at 1163.

158. *Cf. supra* note 152 and accompanying text.

159. *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words . . . .").

160. *Cf. supra* notes 29–30 (reviewing analogous examples of website redirects that criticize the target).

liver an obscure message of disapproval. This is analytically similar to a picket or protest in physical space where the cyberattack operates as a means to (1) occupy "adjacent" cyberspace to the place of business of the target and (2) deliver a message through digital placards in the form of pop-up windows.[161] Thus, a cyberattack that generates a pop-up window is likely to qualify as symbolic speech as long as the window delivers a message regarding the protest to the visitor of the target's website.

Furthermore, a cyberattack that generates a pop-up window is not censorial in nature. It does not take down the target's website but rather incorporates its own message into the website in the form of a pop-up window that has a positive net impact on public discourse. Pop-up windows, in effect, operate like website redirects, but instead of replacing one set of expression with that of another, pop-up windows still permit the visitors to view the content on the targeted website. Furthermore, this kind of tactic is likely to generate more speech as the target may feel compelled to respond directly on its website, and the hacktivists have a fuller opportunity to express themselves through the pop-up window, which has the capacity to contain a compelling narrative or other well-crafted content embedded within the window. Thus, unlike other potentially censorial forms of cyberattack, cyberattacks that generate pop-up windows would in fact further First Amendment interests.

D. Content-Neutral Restrictions

Even if a particular form of cyberattack is deemed to fall within the protection of the First Amendment, it may still be subject to content-neutral restrictions. The government can regulate the *means* used to deliver protected online speech just as the government can regulate the use of loud speakers that disruptively broadcast protected speech.[162] Whereas content-based regulations are subject to strict scrutiny, content-neutral regulations are subject to only intermediate scrutiny under the *O'Brien* test.[163]

---

161. *But see* Rumsfeld v. Forum for Academic & Institutional Rights, Inc., 547 U.S. 47, 66 (2006) ("The expressive component of a law school's actions is not created by the conduct itself but by the speech that accompanies it. The fact that such explanatory speech is necessary is strong evidence that the conduct at issue here is not so inherently expressive that it warrants protection . . . .").

162. *Cf.* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

163. *See* United States v. O'Brien, 391 U.S. 367, 376–77 (1968); *see also* Texas v. Johnson, 491 U.S. 387, 406–07 (1989). The government can regulate non-communicative aspects of symbolic speech if: (1) the regulation is within the constitutional power of the government, (2) the regulation furthers an important governmental interest, (3) the governmental interest is unrelated to the suppression of free speech, and (4) the incidental restriction of First Amendment freedoms is no greater than essential to furthering the governmental interest. *O'Brien*, 391 U.S. at 376–77.

Because the CFAA regulates a means of expression (i.e., technology hacking), the law is content-neutral and likely meets the *O'Brien* test.[164] However, the CFAA's categorical ban on cyberattacks effectively deprives speakers of a unique form of protected speech, which requires assertion in cyberspace to gain specific access to a relevant audience. As discussed above, specific locations are sometimes critical for reaching the particular audience that the speaker is seeking to influence.[165] Furthermore, the uniqueness of the regulated channel of communication is particularly prominent in this case, taking into consideration the discussion in Section IV.B regarding cyberspace as an alternative to — rather than extension of — physical space.

As our daily activities increasingly extend into cyberspace, the interests underlying the First Amendment that require tolerance of protests in the physical world demand that the same protection extend to their digital equivalents. Although not all forms of hacktivism would be protected by the First Amendment, the law should adapt to recognize those socially productive forms of hacktivism that further First Amendment purposes in cyberspace. A narrower regulation would significantly reduce the negative impact on protected speech as compared to the CFAA's existing categorical ban. The government could continue to prohibit the forms of cyberattacks that are censorial in nature or lacking in expression while crafting the statute more narrowly to permit cyberattacks that generate qualifying pop-up windows. For example, the CFAA could provide exemptions for cyberattacks that generate qualifying pop-up windows, which must meet restrictions in terms of size, position, opt-in/opt-out, etc. to minimize the intrusion into the web browsing experience.

V. CONCLUSION

Heralded as the "largest online protest,"[166] on January 18, 2012, popular websites such as Wikipedia and Reddit "blacked out" their webpages in protest of the Stop Online Piracy Act ("SOPA") before Congress.[167] In lieu of their normal functions, participating websites posted messages explaining the black out as a means to raise aware-

164. Content-neutral regulations tend to be upheld and First Amendment defenses tend to be rejected by the Supreme Court under the lax level of scrutiny prescribed by the *O'Brien* test. *See* Ashutosh Bhagwat, *The Test that Ate Everything: Intermediate Scrutiny in First Amendment Jurisprudence*, 2007 U. ILL. L. REV. 783, 789 (2007).

165. *See* Zatz, *supra* note 133, at 224. *See also* City of Erie v. Pap's A.M., 529 U.S. 277 (2000) (considering whether the regulation of expressive conduct leaves ample alternatives under *O'Brien*).

166. *The January 18 Blackout/Strike*, SOPA STRIKE, http://www.sopastrike.com/numbers (last visited Dec. 20, 2013).

167. Timothy B. Lee, *Wikipedia to Join Reddit in SOPA Blackout Wednesday*, ARS TECHNICA (Jan. 16, 2012, 2:45 PM), http://arstechnica.com/tech-policy/2012/01/wikipedia-to-join-reddit-in-sopa-blackout-wednesday.

ness for the anti-SOPA cause and rally users to get in touch with their respective congressmen.[168] By the end of the day, eighteen senators had defected to the side opposing the bill,[169] six of whom were the original sponsors of the bill.[170] The anti-SOPA blackout has proven cyber protests can be "swift and astoundingly successful."[171]

While shutting down websites as a form of cyber-protest proved highly effective in the anti-SOPA blackout, such action is largely unavailable to individual citizens who lack the private resources to have a popular website shut down at their beckoning. Hacktivism offers everyday citizens the ability to gain specific access in cyberspace to target websites, whereby the target of protest "cannot avoid being targeted by virtue of its power or its location, or a people's poverty or oppression." [172] Cyberattacks that generate pop-up windows raise the possibility of First Amendment protection, but the low level of scrutiny afforded to content-neutral regulations such as the CFAA may continue to present a barrier. Ultimately, a legal reconceptualization of cyberspace will be needed to adequately safeguard socially productive forms of hacktivism against unwarranted prosecution.

168. SOPA STRIKE, *supra* note 166.

169. Athima Chansanchai, *Wikipedia Traffic Surged During SOPA Blackout*, NBC NEWS (Jan. 19, 2012, 11:06 AM), http://www.nbcnews.com/technology/technolog/wikipedia-traffic-surged-during-sopa-blackout-117767.

170. *See, e.g.*, Jim Abrams, *Wikipedia SOPA Blackout Seems to Get Results in Senate*, CHICAGO SUN-TIMES (Jan. 19, 2012, 5:28 PM), http://www.suntimes.com/business/10111729-420/wikipedia-sopa-blackout-seems-to-get-results-in-senate.html.

171. *SOPA Blackout: 5 Reasons Why It Worked*, GLOBAL POST (Jan. 19, 2012, 5:13 PM), http://www.globalpost.com/dispatch/news/regions/americas/united-states/120119/sopa-blackout-protest-yields-results; *see also* Matt Peckham, *Did It Work? 'Day After' Results of the SOPA, PIPA Blackout*, TIME (Jan. 19, 2012), http://techland.time.com/2012/01/19/did-it-work-day-after-results-of-the-sopa-pipa-blackout.

172. *See* Hampson, *supra* note 24, at 542.