NOTES

BLURRED LINES OF IDENTITY CRIMES: INTERSECTION OF THE FIRST AMENDMENT AND FEDERAL IDENTITY FRAUD

*Philip F. DiSanto**

Several recent high-profile criminal cases have highlighted the dynamic nature of identity crimes in a modern digital era and the boundaries prosecutors sometimes push to squeeze arguably wrongful conduct into an outdated legal framework. In many cases, two federal statutes—18 U.S.C § 1028 and § 1028A—provide prosecutors with potent tools to aggressively pursue online identity thieves. But the broadly defined terms of these provisions may also expose innocent parties to criminal liability.

This Note argues that broadly defined federal identity-fraud statutes facilitate unconstitutional restrictions on protected speech. Specifically, this Note maintains that § 1028 and § 1028A are defined in vague and overbroad statutory terms that criminalize expressive conduct and chill protected speech. Left unchecked, these statutes expose institutional journalists, online commentators, and ordinary citizens to criminal liability for nothing more than sharing a hyperlink. This Note then concludes by presenting three potential routes to eliminate these unconstitutional restrictions and protect the Internet's role as a unique communication medium.

INTRODUCTION

On September 12, 2012, the Federal Bureau of Investigation (FBI) took Barrett Brown into custody in Dallas, Texas.[1] Law-enforcement officers raided his apartment several hours after he posted a video threatening to "destroy" the life of a federal agent and gather information about that agent's family.[2] The FBI had previously searched both his apartment and his mother's apartment in the weeks leading up to his

* J.D. Candidate 2015, Columbia Law School.

1. See Gerry Smith, Barrett Brown Arrested: Former Anonymous Spokesman Taken into Custody After Threatening FBI Agent, Huffington Post (Sept. 13, 2012, 7:23 PM), http://www.huffingtonpost.com/2012/09/13/barrett-brown-arrested-fo_n_1881535.html (on file with the *Columbia Law Review*) (discussing factual circumstances surrounding Brown's arrest).

2. Id.; Barrett Brown, Why I'm Going to Destroy FBI Agent [RS] Part Three, YouTube (Sept. 12, 2012), http://youtu.be/TOW7GOrXNZI [hereinafter Brown YouTube Video] (on file with the *Columbia Law Review*).

arrest due to his alleged involvement in the dissemination of confidential personal information gleaned from documents posted by an individual affiliated with the hacker collective known as "Anonymous."[3] Prosecutors initially charged Brown with making internet threats against a federal agent, threatening to disseminate restricted personal information about a federal agent, and retaliating against a federal law-enforcement officer.[4]

Two months later, prosecutors also charged Brown with an additional fourteen identity-fraud counts, including trafficking in stolen authentication features, access device fraud, and aggravated identity theft.[5] The government claimed Brown committed federal identity fraud and aggravated identity theft by copying a hyperlink to the infringing documents and sending that hyperlink to a group of individuals in a chat room under his control.[6] While awaiting trial in Texas, he faced a maximum sentence of 105 years in prison.[7]

It would be difficult to characterize Barrett Brown as a sympathetic figure.[8] The cause for his initial arrest—a series of videos posted on

---

3. See Peter Ludlow, The Strange Case of Barrett Brown, Nation (June 18, 2013), http://www.thenation.com/article/174851/strange-case-barrett-brown (on file with the *Columbia Law Review*) (discussing factual background of case against Barrett Brown); see also Glenn Greenwald, The Persecution of Barrett Brown—And How to Fight It, Guardian (Mar. 21, 2013, 10:15 AM), http://www.theguardian.com/commentisfree/2013/mar/21/barrett-brown-persecution-anonymous (on file with the *Columbia Law Review*) (providing timeline of FBI searches of Brown's residences). For background on the hacking collective Anonymous, see generally David Kushner, The Masked Avengers: How Anonymous Incited Online Vigilantism from Tunisia to Ferguson, New Yorker (Sept. 8, 2014), available at http://www.newyorker.com/magazine/2014/09/08/masked-avengers (on file with the *Columbia Law Review*).

4. See Indictment at 7–9, United States v. Brown, No. 3:12-CR-00317 (N.D. Tex. Oct. 3, 2012) [hereinafter Brown First Indictment] (enumerating charges against Brown in original indictment).

5. See Indictment at 1–3, United States v. Brown, No. 3:13-CR-00030 (N.D. Tex. Jan. 23, 2013) [hereinafter Brown Second Indictment] (enumerating concealment of evidence charges); Superseding Indictment at 1–5, United States v. Brown, No. 3:12-CR-00413 (N.D. Tex. Jul. 2, 2013) [hereinafter Brown Third Indictment] (enumerating federal identity-fraud charges).

6. See Brown Third Indictment, supra note 5, at 1 (enumerating concealment of evidence and obstruction of justice charges); see also Press Release, U.S. Dep't of Justice, Dallas Man Associated with Anonymous Hacking Group Faces Additional Federal Charges (Dec. 7, 2012), http://www.justice.gov/usao/txn/PressRelease/2012/DEC2012/dec7brown_barrett_ind.html (on file with the *Columbia Law Review*) (explaining details of IRC channels to which hyperlink was shared).

7. See Kevin Drum, 105 Years in Jail for Posting a Link?, Mother Jones (Sept. 9., 2012, 11:47 AM), http://www.motherjones.com/kevin-drum/2013/09/barrett-brown-105-years-jail-posting-link (on file with the *Columbia Law Review*) (discussing maximum prison sentence for each of Brown's counts); Patrick McGuire, Why Is Barrett Brown Facing 100 Years in Prison?, VICE News (Feb. 1, 2013), http://www.vice.com/read/why-is-barrett-brown-facing-100-years-in-jail (on file with the *Columbia Law Review*) (same).

8. See, e.g., Michael Isikoff, Hacker Group Vows 'Cyberwar' Against US Government, Business, NBC News (Mar. 8, 2011, 6:28 PM), http://www.nbcnews.com/id/41972190/ns/technology_and_science-security/t/hacker-group-vows-cyberwar-us-

YouTube in which he threatens an FBI agent for searching his home[9]—does little to support his case. However, the unique circumstances of his prosecution reveal weaknesses in the federal identity-fraud regime that affect more than just bloggers with questionable journalistic credentials.[10] Originally enacted to combat the proliferation of fraudulent immigration documents and later amended in response to online trading in stolen credit card information,[11] the federal identity-fraud statutes employ extraordinarily broad terms. While such open-ended phrasing gives law enforcement and prosecutors powerful tools to pursue identity thieves,[12] Brown's prosecution demonstrates that even the relatively innocuous act of copying and pasting a hyperlink may constitute federal identity fraud.[13]

This Note argues that several broad provisions of the federal identity-fraud statutes may facilitate unconstitutional restrictions on protected speech. Part I provides background information on identity fraud in the United States and discusses recent challenges related to hacktivism and dumps of confidential documents. Part II explores how federal identity-fraud statutes may restrict protected speech. Specifically, Part II.A presents an overview of First Amendment doctrine as applied to federal identity fraud. Part II.B examines two perspectives one might take

---

government-business/ (on file with the *Columbia Law Review*) (observing Brown's involvement in self-proclaimed "guerrilla cyberwar" against United States, among others).

9. Brown YouTube Video, supra note 2.

10. See infra notes 78–88 and accompanying text (discussing factual circumstances of Brown's case); infra Part II.B (discussing potential restrictions on protected speech imposed by identity-fraud statutes).

11. See infra Parts I.A–B (discussing evolution of identity fraud and identity theft under federal law).

12. Though some might argue aggressive prosecution using the federal identity-fraud statutes falls within prosecutorial discretion (and thereby avoids some of the tougher questions about fundamental rights), others have recognized the serious problems with overcriminalization and unconstrained discretion in the modern era. E.g., Glenn Harlan Reynolds, Ham Sandwich Nation: Due Process When Everything Is a Crime, 113 Colum. L. Rev. Sidebar 102, 103–04 (2013), http://columbialawreview.org/ham-sandwich-nation_reynolds/. Problems with prosecutorial discretion—though clearly underlying the Brown case and computer-crime prosecutions generally—will not be addressed directly in this Note.

13. The Department of Justice eventually dropped all identity-fraud charges against Brown and prosecuted him based solely on threats against a federal law-enforcement officer and aiding and abetting computer fraud. See Kim Zetter, Barrett Brown Signs Plea Deal in Case Involving Stratfor Hack, Wired (Apr. 3, 2014, 2:30 PM), http://www.wired.com/2014/04/barrett-brown-plea-agreement/ (on file with the *Columbia Law Review*) (discussing Brown's plea agreement and development of charges against him). Brown signed a sealed plea agreement excluding identity-fraud charges, see Superseding Information at 1–3, United States v. Brown, No. 3:12-CR-413-L (N.D. Tex. Mar. 31, 2014), and was recently sentenced to sixty-three months imprisonment on the remaining charges. Kim Zetter, Barrett Brown Sentenced to 5 Years in Prison in Connection to Stratfor Hack, Wired (Jan. 22, 2015, 2:43 PM), http://www.wired.com/2015/01/barrett-brown-sentenced-5-years-prison-connection-stratfor-hack/ (on file with the *Columbia Law Review*).

in approaching First Amendment challenges to identity-fraud statutes and argues for heightened scrutiny in certain circumstances. Part II.C also highlights ambiguities in the Supreme Court's recent First Amendment doctrine concerning dissemination of information unlawfully obtained by third parties. Part III then concludes by proposing three methods to eliminate or avoid unconstitutional restrictions on protected speech.

I. PROSECUTING IDENTITY FRAUD IN THE DIGITAL AGE

A. *Prevalence of Identity Fraud*

The evolution of the Internet and digital content over the past two decades has dramatically altered the nature of identity crimes and investigative approaches taken by law enforcement.[14] While federal identity-fraud statutes originally targeted more traditional identity crimes[15]—such as producing fake driver's licenses—subsequent amendments to these statutes clearly cover online and digital fraud as well.[16] Rapid evolution in both technology and the statutory framework has resulted in serious questions of statutory construction,[17] intent requirements,[18] and federal law-enforcement priorities.[19] Some of these challenges are discussed in greater depth throughout the remainder of Part I.

---

14. See infra notes 16–23 and accompanying text (discussing law-enforcement response to more advanced identity crimes and changes in technology and techniques).

15. See infra Part I.B (discussing purposes of 1998 and 2003 amendments to § 1028).

16. 18 U.S.C. § 1028(d)(1) (2012) (defining "authentication feature" as "any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature" used to determine whether identification document is "counterfeit, altered, or otherwise falsified"); id. § 1028(d)(7) (defining "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual").

17. The breadth of the statutory terms provided by § 1028(d) has led the Department of Justice to assert even possession or distribution of email addresses may constitute identity fraud when those email addresses are fraudulently obtained. See, e.g., Brief for Appellee at 65–66, United States v. Auernheimer, 748 F.3d 525 (3d Cir. Sept. 20, 2013) (No. 13-1816) (arguing use of individual's email address may constitute identity fraud when used with intent to obtain unauthorized access); see also Brief of Amici Curiae Mozilla Foundation, Computer Scientists, Security and Privacy Experts in Support of Defendant-Appellant and Reversal at 4–7, *Auernheimer*, 748 F.3d 525 (3d Cir. Jul. 8, 2013) (No. 13-1816) (expressing concerns of privacy and security experts regarding broadly defined computer-fraud crimes and liability for incrementing public URL).

18. See, e.g., Flores-Figueroa v. United States, 556 U.S. 646, 657 (2009) (holding conviction for aggravated identity theft requires knowledge that means of identification belong to another person).

19. See The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan 13–15 (2007), available at http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (on file with the *Columbia Law Review*) (discussing federal enforcement priorities and identity-fraud trends).

1. Evolution of Identity Crimes. — Though more traditional forms of identity fraud such as dumpster diving and passport forgery remain legitimate security concerns,[20] digital content and the Internet have fundamentally changed the nature of identity crimes. Over the past two decades, a massive amount of personal-identity information has been transferred to electronic storage mediums—generally those connected to the Internet. E-commerce websites process credit cards when online purchases are made, banks record financial transactions in networked databases, and the government has made it easier to file tax returns with the click of a mouse.[21] This greater availability of information has resulted in lucrative opportunities for identity thieves.[22]

Online identity fraud takes many forms and is facilitated by constantly evolving techniques. For example, before implementation of sophisticated verification technology, skilled hackers frequently engaged in "carding" schemes, in which fraudulently obtained credit card numbers were sold on internet forums to the highest bidder.[23] Internet-based identity fraud is rarely perpetrated by a single individual; the personal financial consequences that make identity theft so devastating often result only after personal information is filtered through several layers of the online and offline underworld.[24] Sophisticated hackers have become the bridge between legitimate possessors of personal information and

---

20. Id. (describing "dumpster diving" as among most prevalent modern identity-theft techniques).

21. See Kurt M. Saunders & Bruce Zucker, Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act, 8 Cornell J.L. & Pub. Pol'y 661, 661 (1999) (discussing Internet boom and development of electronic commercial transactions); see also Andreas Meier & Henrik Stormer, eBusiness & eCommerce 126–28 (2009) (discussing ePayment systems and drawbacks of credit card use in eCommerce); Free File: Do Your Federal Taxes for Free, IRS, http://www.irs.gov/uac/Free-File:-Do-Your-Federal-Taxes-for-Free (on file with the *Columbia Law Review*) (last visited Mar. 5, 2015) (providing step-by-step instructions for filing federal tax forms online).

22. See Saunders & Zucker, supra note 21, at 675 ("With the onset of the information age, the fundamental ability to protect one's personal information and identity is now more in jeopardy than ever.").

23. See, e.g., Kevin Poulsen, One Hacker's Audacious Plan to Rule the Black Market in Stolen Credit Cards, Wired (Dec. 22, 2008), http://www.wired.com/techbiz/people/magazine/17-01/ff_max_butler [hereinafter Poulsen, Black Market] (on file with the *Columbia Law Review*) (discussing massive "carding" scheme facilitated by hacker Max Ray Butler).

24. Sophisticated hackers are frequently responsible for initial data breaches facilitating identity theft but not for direct misuse of individuals' exposed credit card numbers and personal information. See id. (explaining how, in early 2000s, "identity thief in Denver could buy stolen credit card numbers from a hacker in Moscow, send them to Shanghai to be turned into counterfeit cards, then pick up a fake driver's license from a forger in Ukraine before hitting the mall"). This division of labor also appears to have been manifest in the Stratfor leak, as a small group of hackers penetrated private systems and passed confidential information on to a larger group of individuals. See infra notes 82–88 and accompanying text (discussing Stratfor leak and involvement of key players).

identity thieves lacking the technical skills necessary to steal valuable identity information. Once personal information is dumped online or sold to downstream fraudsters, that information is misused to make fraudulent purchases or stashed away for other criminal purposes.[25]

2. Law-Enforcement Barriers and Fraud Prevention. — The Internet has also made it much more difficult to investigate and prosecute computer-based identity fraud.[26] Digital communication provides a degree of anonymity: Tech-savvy users often identify themselves with nothing more than a forum handle. While criminals sometimes fail to conceal their true identities,[27] the massive resources required by identity-fraud investigations often prevent agencies from pursuing small-scale fraudsters.[28] Law-enforcement strategies have therefore focused on prevention and mitigation, as opposed to investigating isolated incidents.[29] These strategies focus on decreasing the availability of sensitive personal information on public-facing websites, increasing citizen awareness of identity fraud, and enforcing stricter requirements regarding data retention and encryption.[30]

---

25. Poulsen, Black Market, supra note 23; see also The President's Identity Theft Task Force, supra note 19, at 13 (discussing different actors in identity-fraud scams and burgeoning marketplace for malicious software tools). Identity information is also used to obtain unauthorized access, establish new lines of credit, circumvent immigration laws, and establish strong brokering positions with other online criminals. Id. at 18–21.

26. See Robert Strang, Recognizing and Meeting Title III Concerns in Computer Investigations, U.S. Att'ys' Bull. (U.S. Dep't of Justice, Washington, D.C.), Mar. 2001, at 8, 8–9, available at http://www.justice.gov/sites/default/files/usao/legacy/2006/06/30/usab4902.pdf (on file with the *Columbia Law Review*) (discussing difficulty of prosecuting computer criminals and proliferation of "anonymizers" as law-enforcement barriers).

27. See, e.g., Nate Anderson & Cyrus Farivar, How the Feds Took Down the Dread Pirate Roberts, Ars Technica (Oct. 3, 2013, 12:00 AM), http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/ (on file with the *Columbia Law Review*) (discussing apprehension of notorious "Dread Pirate Roberts," administrator of illegal online marketplace and his failure to conceal his true identity).

28. See U.S. Gen. Accounting Office, GAO/GGD-98-100BR, Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited 29 (1998) (providing rapidly growing investigative cost figures for U.S. Secret Service); see also The President's Identity Theft Task Force, supra note 19, at 58–59 (discussing coordination with foreign law enforcement and barriers to international identity-fraud investigations); Ed Dadisho, Identity Theft and the Police Response, Police Chief (Jan. 2005), available at http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=493&issue_id=12005 (on file with the *Columbia Law Review*) (discussing personnel issues in identity-theft investigations by local police).

29. See The President's Identity Theft Task Force, supra note 19, at 62–63 (recognizing limited financial resources to prosecute identity theft and discussing "monetary thresholds" at which U.S. Attorneys' Offices will pursue cases).

30. See, e.g., id. at 22–44 (discussing public-sector strategies for identity-theft prevention and harm mitigation); see also PCI Sec. Standards Council, Data Security Standard: Requirements and Security Assessment Procedures 5 (2010), available at https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf (on file with the *Columbia Law Review*) (providing private-sector data security standards for protection of consumer information and, specifically, credit card information).

B. *Identity Fraud Under Sections 1028 and 1028A*

The legal framework for identity fraud in the United States is a complicated patchwork of state and federal statutes.[31] Identity and fraud-related crimes under federal law are exceptionally varied—the government may charge an individual with access device fraud,[32] computer fraud,[33] mail fraud,[34] wire fraud,[35] financial institution fraud,[36] and immigration document fraud,[37] each under different provisions of the United States Code.[38] Beyond those activities criminalized by federal statute, individuals may also face criminal penalties under more comprehensive state codes.[39]

The government prosecutes a majority of federal identity-fraud cases under a general identity-fraud statute, 18 U.S.C. § 1028,[40] and the more recently enacted aggravated identity-theft statute, 18 U.S.C. § 1028A.[41] Congress has amended this framework on several occasions, responding to changes in technology and public pressure.[42] Originally enacted as part of the False Identification Crime Control Act of 1982, § 1028 targeted the fraudulent production, transfer, or possession of "identification documents."[43] Congress was targeting the production of counterfeit physical documents used to misrepresent one's identity in response to the

31. See U.S. Dep't of Justice, A National Strategy to Combat Identity Theft 28–29 (2006) (discussing need to document state and federal identity-fraud statutes in accessible format); see also infra notes 38–47 (detailing state and federal identity-fraud statutes).

32. 18 U.S.C. § 1029 (2012).

33. Id. § 1030.

34. Id. § 1341.

35. Id. § 1343.

36. Id. § 1344.

37. Id. § 1546.

38. See Sean B. Hoar, Identity Theft: The Crime of the New Millennium, U.S. Att'ys' Bull. (U.S. Dep't of Justice, Washington, D.C.), Mar. 2001, at 14, 17–18, available at http://www.justice.gov/sites/default/files/usao/legacy/2006/06/30/usab4902.pdf (on file with the *Columbia Law Review*) (discussing various federal identity-theft statutes).

39. See, e.g., Cal. Penal Code §§ 528–539 (West 2010 & Supp. 2014) (enumerating identity-theft crimes in California); N.Y. Penal Law § 190.77–.86 (McKinney 2010 & Supp. 2014) (enumerating identity-theft crimes in New York).

40. 18 U.S.C. § 1028 (prohibiting fraud related to "identification documents," "authentication features," "means of identification," and "document-making implement[s]").

41. Id. § 1028A (prohibiting "aggravated identity theft"—defined as "knowingly transfer[ring], possess[ing], or us[ing], without lawful authority, a means of identification of another person" in connection with enumerated felony—and providing mandatory sentence "to a term of imprisonment of 2 years" for each offense).

42. See infra Part II.B.1–2 (discussing amendments to § 1028 and enactment of § 1028A).

43. See False Identification Crime Control Act of 1982, Pub. L. No. 97-398, 96 Stat. 2009 (prohibiting production, transfer, or possession of fraudulent identification documents and document-making implements known to be used for production of fraudulent documents).

proliferation of physical reproduction technology.[44] Increasingly sophisticated reproduction technology and criminal implementations of that technology have resulted in several amendments to § 1028,[45] as well as the enactment of minimum sentencing requirements under § 1028A for certain felony offenses.[46]

Identity *theft* was not explicitly made a federal crime until 1998, when Congress amended § 1028 with the Identity Theft and Assumption Deterrence Act of 1998 (ITADA) in response to increased public pressure and the migration of financial information to digital and online media.[47] The scope of prohibited conduct distinguishes identity theft from identity fraud; while identity-fraud provisions criminalize a broad range of fraudulent behavior, identity theft targets the victimization of specific individuals.[48] The ability to conduct sensitive transactions on the Internet enabled criminals to impersonate others for financial gain, resulting in correspondingly personal harm to the victim.[49]

In adding § 1028(a)(7) as an identity-fraud offense, Congress appears to have been responding to this growing threat to individual citi-

---

44. See 144 Cong. Rec. 24,379–84 (1998) (discussing gaps in federal identity-fraud statutes because Congress only criminalized fraudulent production, use, or transfer of identity *documents* prior to Identity Theft and Assumption Deterrence Act of 1998); see also H.R. Rep. No. 97-975, at 1–3 (1982), available at http://congressional.proquest.com/congressional/docview/t49.d48.13489_h.rp.802?accountid=10226 (on file with the *Columbia Law Review*) (discussing purpose of False Identification Crime Control Act of 1982 as need to prevent production and use of fraudulent identification for use in drug smuggling and immigration offenses).

45. See infra notes 47–56 (discussing Identity Theft and Assumption Deterrence Act of 1998 and SAFE ID Act of 2003).

46. See 18 U.S.C. § 1028A(a)(1) (imposing two-year sentence for committing one of several enumerated violations).

47. See Identity Theft and Assumption Deterrence Act of 1998, Pub L. No. 105-318, § 3(a)(4), 112 Stat. 3007, 3007 (codified at 18 U.S.C. § 1028(a)(7)) (criminalizing unlawful transfer or use of "means of identification of another person with intent to commit . . . unlawful activity"); see also id. § 3(d) (defining "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual" and providing list of examples).

48. See Kristin M. Finklea, Cong. Research Serv., R40599, Identity Theft: Trends and Issues 2 (2014), available at http://fas.org/sgp/crs/misc/R40599.pdf (on file with the *Columbia Law Review*) (discussing identity theft, aggravated identity theft, and concerns with victimization); id. at 27 (observing significant increase in amount of personal data stored online impacts nature of identity crimes and contributes to dangers of individual identity theft).

49. See S. Rep. No. 105-274, at 7 (1998) (discussing evolving threat of identity fraud using internet). Compelling personal anecdotes often provided impetus at both the state and federal levels. See, e.g., Michael Kiefer, Bob Hartle's Identity Crisis, Phx. New Times (Apr. 24, 1997), http://www.phoenixnewtimes.com/1997-04-24/news/bob-hartle-s-identity-crisis/ (on file with the *Columbia Law Review*) (discussing particularly egregious case in which Arizona authorities were unable to prosecute identity thief due to absence of statutory prohibition); see also Finklea, supra note 48, at 4 n.16 (stating Arizona passed first identity-theft statute in 1996).

zens.[50] During debate in the House of Representatives, comments focused on the ease with which a malicious individual could obtain and abuse another's personal information, as well as on the financial hardship that victims faced due to gaps in federal law.[51] Representatives also focused on the Internet's impact on the availability of personal information; because the Internet makes information more accessible, identity crimes were becoming more widespread.[52] Yet, despite Congress's concern for struggling individuals, critics remained skeptical that amendments to § 1028 would alleviate the financial burdens of identity theft due to a lack of funding for federal investigations.[53] Furthermore, despite explicitly criminalizing "identity theft," Congress initially failed to provide enhanced penalties corresponding to the severity of these crimes.[54]

Congress also recognized in the early 2000s that concerns regarding identity authentication had expanded beyond the realm of physical documents and digital "means of identification."[55] The SAFE ID Act of 2003 expanded the language of § 1028 to prohibit fraudulent production, transfer, or possession of "authentication features" such as holograms and watermarks.[56] Though this prohibition clearly covers authentication features such as a driver's license hologram or birth-certificate watermark, the definition of "authentication features" is also broad enough to cover any string of numbers or letters used for authentication purposes.[57]

---

50. See S. Rep. No. 105-274, at 7 (referring to "[f]inancial crimes involving the misappropriation of *individuals*' identifying information" and noting "devastating" effects of identity theft on individual victims (emphasis added)).

51. See 144 Cong. Rec. 24,379–84 (1998) (debating purpose and utility of Identity Theft and Assumption Deterrence Act of 1998).

52. Id. at 24,384 (statement of Rep. Sanders) (discussing dangers posed by readily available personal-identity information on Internet).

53. See, e.g., Martha A. Sabol, The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?, 11 Loy. Consumer L. Rev. 165, 169 (1999) (noting lack of federal funding in ITADA forced federal authorities to continue concentrating on large identity scams).

54. See 18 U.S.C. § 1028(b) (1988) (failing to differentiate between identity theft and other identity crimes for sentencing purposes). This failure to provide heightened penalties for identity theft was partially addressed by consecutive minimum sentences imposed by § 1028A. 18 U.S.C. § 1028A(b) (2012).

55. 18 U.S.C. § 1028(a)(7) (prohibiting "knowingly transfer[ring], possess[ing], or us[ing], without lawful authority, a means of identification of another person").

56. SAFE ID Act, Pub. L. No. 108-21, § 607, 117 Stat. 689 (2003) (codified as amended at 18 U.S.C. § 1028); see also id. § 607(b)(4)(B) (defining "authentication feature" as "any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that . . . is used by the issuing authority on an identification document . . . or means of identification to determine if the document is counterfeit, altered, or otherwise falsified").

57. Id. (defining "authentication feature" as including "any . . . sequence of numbers or letters").

Despite the breadth of the SAFE ID Act's amendments, there appears to have been little congressional debate regarding the amendment.[58]

C. *Hacktivism and Identity Crimes*

The practice of dumping massive numbers of confidential and personal documents on the Internet has resulted in recent challenges for identity-fraud investigators and prosecutors. For example, an online hacktivist group,[59] referring to itself as "LulzSec," made waves in the data-security and law-enforcement communities by breaching private systems and dumping confidential personal information on the Internet in late 2011.[60] Unlike criminal syndicates or lone-wolf hackers who breach systems for profit, LulzSec appears to have facilitated massive data breaches for entertainment value and the embarrassment of its targets.[61] However, even in circumstances where LulzSec members did not themselves exploit personal information, they often posted this information online and made it available on public file-sharing websites.[62]

---

58. See 149 Cong. Rec. S5388 (daily ed. Apr. 11, 2003) (reflecting limited debate on SAFE ID Act); 149 Cong. Rec. H2440–43 (daily ed. Mar. 27, 2003) (same).

59. "Hacktivism" refers to hacking in support of a political, economic, or social agenda. The term was first used in the late 1990s, when several groups turned to hacking as a means of furthering political agendas. See Amy Harmon, 'Hacktivists' of All Persuasions Take Their Struggle to the Web, N.Y. Times (Oct. 31, 1998), http://www.nytimes.com/1998/10/31/world/hacktivists-of-all-persuasions-take-their-struggle-to-the-web.html (on file with the *Columbia Law Review*) (discussing hacking efforts by political groups opposed to Mexican government, Indian nuclear testing, and Kosovo independence).

60. See LulzSec, Twitter (May 6, 2011, 7:36 PM), https://twitter.com/LulzSec/status/66647480388956160 (on file with the *Columbia Law Review*) (taking credit for hacking Fox.com and releasing contestant databases); see also Sealed Indictment at 2, 6–7, United States v. Ackroyd, No. 1:12-CR-00185 (S.D.N.Y. Feb. 27, 2012), 2012 WL 716070 [hereinafter Ackroyd Indictment] (discussing LulzSec infiltration of HBGary Federal using name "Internet Feds"); Matt Liebowitz, Hackers Leak Fox.com Employee Info, NBC News (May 13, 2011, 8:15 PM), http://www.nbcnews.com/id/43027482/ns/technology_and_science-security/t/hackers-leak-foxcom-employee-info/ (on file with the *Columbia Law Review*) (detailing LulzSec Fox.com hack).

61. See Andrew Morse & Ian Sherr, For Some Hackers, Goal Is Pranks, Wall St. J. (June 6, 2011), http://online.wsj.com/news/articles/SB10001424052702304906004576367870123614038 (on file with the *Columbia Law Review*) (arguing LulzSec focused on hacking as attention-garnering pranks); Parmy Olson, Hacker Group Raids Fox.com, Targets FBI, Forbes (May 10, 2011, 2:51 PM), http://www.forbes.com/sites/parmyolson/2011/05/10/hacker-group-raids-fox-com-targets-fbi/ (on file with the *Columbia Law Review*) (exploring motivation for LulzSec Fox.com hack).

62. See Suzanne Choney, LulzSec Download Carried Trojan, NBC News (June 28, 2011, 8:57 AM), http://technolog-discuss.nbcnews.com/_news/2011/06/28/8964687-lulzsec-download-carried-trojan?d=1 (on file with the *Columbia Law Review*) (discussing LulzSec's final post on The Pirate Bay); Elinor Mills, LulzSec Releases Arizona Law Enforcement Data, CNET News (June 23, 2011, 4:46 PM), http://news.cnet.com/8301-27080_3-20073843-245/lulzsec-releases-arizona-law-enforcement-data/ (on file with the *Columbia Law Review*) (reporting LulzSec attack on Arizona Department of Public Safety and subsequent release of confidential documents on The Pirate Bay); Olson, supra note

LulzSec's campaign of infiltration and information dumping has become characteristic of a new pattern in online mischief and identity fraud. Small groups of hackers with exceptional technical expertise lead many modern cyberattacks; these individuals exploit systems to damage, deface, or steal information.[63] But skilled hackers are often surrounded by a larger group of followers who exploit information released or who only passively participate in targeted attacks.[64] High-profile cyberattacks also draw digital onlookers and supporters without technical skills; this group may include security bloggers, political activists, institutional journalists, and ordinary citizens.[65] Existing laws, including federal identity- and computer-fraud statutes, often fail to account for this diversity of motives and varying degrees of involvement in fraudulent activities, resulting in potentially equal exposure to liability for each of the above groups.

1. Prosecuting Hacktivists Under the Computer Fraud and Abuse Act. — Infiltrating private computer systems without authorization may result in criminal liability under several statutes, but the framework for pursuing nontechnical participants, supporters, and observers is unclear. Prosecutors may invoke several federal statutes to pursue individuals for cyberattack involvement, even when individuals play no role in technical operations. The Computer Fraud and Abuse Act (CFAA),[66] for example, was used to pursue both the skilled hackers behind LulzSec and the group's unofficial spokesperson.[67] The statutory language of the CFAA is rather broad and may be used to prosecute accessing a computer without

---

61 (outlining confidential data posted on The Pirate Bay and explaining LulzSec encouraged followers to "ravage the . . . list of emails and passwords" and "[t]ake from them everything").

63. See Imperva, Imperva's Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack 3 (2012) (observing most Anonymous hacktivist campaigns are led by ten to fifteen highly skilled hackers supported by hundreds of less skilled or unskilled followers).

64. Id. at 3–12 (analyzing timeline of prototypical Anonymous attack, which involved public recruitment, attempts to infiltrate systems and steal data, and subsequent distributed denial-of-service attacks using volunteer network of countless passive supporters).

65. Perhaps the most noteworthy example of this phenomenon is the Steubenville rape case, in which Anonymous dumped information about teenage assailants online and pressured the justice system to pursue further action. Throughout the Steubenville case, members of Anonymous discussed personal information disseminated online with the media. See, e.g., Amanda Marcotte, Rape, Lawsuits, Anonymous Leaks: What's Going On in Steubenville, Ohio?, Slate (Jan. 3, 2013, 2:47 PM), http://www.slate.com/blogs/xx_factor/2013/01/03/steubenville_ohio_rape_anonymous_gets_involved_and_the_case_gets_even_more.html (on file with the *Columbia Law Review*) (describing Anonymous campaign against lack of law-enforcement action in Steubenville rape case and collective's interactions with media).

66. 18 U.S.C. § 1030 (2012).

67. See generally Ackroyd Indictment, supra note 60, at 19–20 (indicting four LulzSec members for violating CFAA); Sealed Indictment at 1–7, United States v. Monsegur, No. 1:11-CR-00666 (S.D.N.Y. Aug. 15, 2011) (indicting Hector Xavier Monsegur, leader of LulzSec, for numerous CFAA violations).

authorization,[68] damaging or threatening to damage a computer,[69] using a computer to commit fraud,[70] or trafficking in passwords and "similar information."[71] The CFAA has also become a potent prosecutorial tool because it explicitly criminalizes conspiracy to commit any of the charges it enumerates.[72]

Critics allege the CFAA defines computer crimes *too* broadly and fails to adapt to modern communications.[73] For example, prosecutors have invoked the CFAA against individuals for violating a website's Terms of Service (TOS)[74] and using an employer's network for activity contrary to the employer's interests.[75] Many of these concerns focus on the CFAA's potential infringement on speech protected under the First Amendment.[76] While the death of Aaron Swartz—an open-access activist who took his own life after being aggressively prosecuted for CFAA violations—recently galvanized calls for CFAA reform, Congress has yet to commit to a major overhaul of the law.[77]

2. Liability for Sharing Confidential Information. — Unlike members of LulzSec, Barrett Brown does not appear to have violated the CFAA.

---

68. 18 U.S.C. § 1030(a)(1)–(6).

69. Id. § 1030(a)(5) (criminalizing intentional or reckless causation of damage to protected computer).

70. Id. § 1030(a)(4) (prohibiting unauthorized access to protected computer with intent to defraud).

71. Id. § 1030(a)(6) (prohibiting trafficking in passwords or "similar information" in connection with unauthorized access to protected computer with intent to defraud).

72. See, e.g., Press Release, FBI, Six Hackers in the United States and Abroad Charged for Crimes Affecting over One Million Victims (Mar. 6, 2012), http://www.fbi.gov/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims (on file with the *Columbia Law Review*) (discussing CFAA charges against skilled LulzSec members and CFAA conspiracy charges against unskilled LulzSec members).

73. See Zoe Lofgren & Ron Wyden, Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act, Wired (June 20, 2013, 9:30 AM), http://www.wired.com/opinion/2013/06/aarons-law-is-finally-here (on file with the *Columbia Law Review*) (arguing CFAA's broad language invites abuse of prosecutorial discretion).

74. See United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (holding breach of website's TOS not actionable offense under CFAA).

75. See, e.g., United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012) (holding defendant not responsible for misusing data from employer's database because it "exceeds authorized access" in CFAA referred to access restrictions).

76. See, e.g., Christine D. Galbraith, Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites, 63 Md. L. Rev. 320, 323 (2004) (discussing potentially unconstitutional overbreadth and vagueness of CFAA).

77. See Lofgren & Wyden, supra note 73 (advocating CFAA reform). According to Senator Ron Wyden and Representative Zoe Lofgren, who coauthored a proposed reform of the CFAA known as "Aaron's Law," the current statute's most significant shortcoming is a failure to distinguish between everyday online activities and "criminals intent on causing serious damage to financial, social, civic, or security institutions." Id.

Though he publicly acknowledges his Anonymous connections, Brown is not seen as one of the more technically skilled individuals associated with the collective.[78] This apparent removal from daily operations of Anonymous did not, however, shield him from criminal charges stemming from the Stratfor Global Intelligence leak in December 2012.[79] Instead of being charged with computer fraud under the CFAA, Brown was indicted for identity fraud, access device fraud, and aggravated identity theft for accessing and sharing a hyperlink to confidential Stratfor documents posted online.[80]

Though legitimate disagreements exist regarding the extent of Brown's involvement with Anonymous and the media's characterization of his case,[81] the basic facts of the Stratfor hack are relatively settled. In December 2011, hacker Jeremy Hammond infiltrated internal Stratfor systems and stole several hundred gigabytes of data including corporate emails, unencrypted credit card numbers, encrypted passwords, and confidential customer lists.[82] Hammond then transferred data to a server in New York and released information via publicly accessible hyperlinks.[83] He was arrested soon thereafter and charged with violations of the CFAA, conspiracy to commit access device fraud, and aggravated identity theft.[84]

---

78. See Tim Rogers, Barrett Brown Is Anonymous, D Mag. (Apr. 2011), http://www.dmagazine.com/publications/d-magazine/2011/april/how-barrett-brown-helped-overthrow-the-government-of-tunisia (on file with the *Columbia Law Review*) (quoting Anonymous source describing Brown as "strong observer[]" of collective's campaigns); see also Kevin M. Gallagher, Barrett Brown, Political Prisoner of the Information Revolution, Guardian (July 13, 2013, 8:00 AM), http://www.theguardian.com/commentisfree/2013/jul/13/barrett-brown-political-prisoner-information-revolution (on file with the *Columbia Law Review*) (discussing Brown's lack of technical skills).

79. See Brown Third Indictment, supra note 5, at 1–5 (discussing twelve charges against Brown related to Stratfor hack).

80. See id. (alleging Brown committed crime by "transferr[ing] the hyperlink . . . [that] provided access to data stolen from the company Stratfor Forecasting Inc.").

81. Federal prosecutors in the Northern District of Texas claim Brown's case has been mischaracterized in the media. See Agreed Order on Extrajudicial Statements at 2, United States v. Brown, No. 3:12-CR-00317-L (N.D. Tex. Sept. 4, 2013) (prohibiting extrajudicial statements by Brown or defense team). Based on the charges in his indictment, however, Brown is not alleged to have participated in the hacking of Stratfor or used the leaked credit card numbers. See Brown Third Indictment, supra note 5, at 1–5 (accusing Brown only of "possess[ing]," "transferring," and "posting" stolen information).

82. See Superseding Information at 2–3, United States v. Hammond, No. 1:12-CR-00185 (S.D.N.Y. May 28, 2013) (presenting factual record on Stratfor hack and CFAA charges against Jeremy Hammond).

83. Id.; see also Kevin Poulsen, Anonymous Hacktivist Jeremy Hammond Pleads Guilty to Stratfor Attack, Wired (May 28, 2013, 3:54 PM), http://www.wired.com/threatlevel/2013/05/hammond-plea/ (on file with the *Columbia Law Review*) (discussing guilty plea in Hammond case).

84. See Superseding Indictment at 27–36, United States v. Ackroyd, No. 1:12-cr-00185 (S.D.N.Y. May 2, 2012) (enumerating charges against Hammond and coconspirators).

Following the Stratfor breach, Brown copied a hyperlink initially posted in an Anonymous IRC channel[85] and pasted that hyperlink in an IRC channel under his own control, allegedly out of interest in the journalistic value of the documents.[86] The hyperlink provided access to Stratfor documents released by Hammond, some of which contained credit card numbers of Stratfor customers.[87] Based on Brown's sharing of the hyperlink, the government claimed:

> [He] knowingly traffic[ked] in more than five authentication features knowing that such features were stolen, in that [he] transferred the hyperlink . . . from the Internet Relay Chat (IRC) called "#Anonops" to an IRC channel under Brown's control called "#ProjectPM," . . . and *by transferring and posting the hyperlink, [he] caused the data to be made available to other persons online*.[88]

Regardless of the outcome in Barrett Brown's own case,[89] commentators and civil rights organizations have referred to the government's interpretation of §§ 1028 and 1028A as troubling for news organizations and journalists that do not fall within traditional definitions.[90] This is due primarily to Brown's arguably journalistic activities. For example, before his legal troubles, Brown was portrayed as an unofficial "spokesperson" for Anonymous.[91] He has also written about his experiences with the collective and frequently discussed their activities with the media.[92] Further complicating matters, Brown had recently emphasized the latter role, distancing himself from Anonymous and portraying himself as an

---

85. An "IRC channel" is a text-based internet messaging protocol commonly used by hacktivist groups due to enhanced controls over access and anonymity. For more technical information, see generally Jarkko Oikarinen & Darren Reed, Internet Relay Chat Protocol, IETF (May 1993), http://tools.ietf.org/pdf/rfc1459.pdf (on file with the *Columbia Law Review*) (presenting technical specifications for IRC protocol).

86. See infra notes 91–93 and accompanying text (discussing claim Brown was seeking information for journalistic value). This claim, however, has been disputed by the government. See Brown Third Indictment, supra note 5, at 1–2 (discussing factual background of Brown's sharing of hyperlink in question).

87. These documents have since been removed from their original location. Redacted versions of the leaked Stratfor documents were subsequently posted on WikiLeaks as "The Global Intelligence Files." See The Global Intelligence Files, WikiLeaks, http://wikileaks.org/the-gifiles.html (on file with the *Columbia Law Review*) (last visited Mar. 8, 2015) (hosting leaked Stratfor documents).

88. Brown Third Indictment, supra note 5, at 1–2 (emphasis added).

89. See supra note 13 (discussing sealed plea agreement in Barrett Brown case).

90. See, e.g., Ludlow, supra note 3 (arguing Brown's prosecution has chilled investigative journalism, particularly with regards to national security and cybersecurity matters).

91. See, e.g., Paul Rexton Kan, Cyberwar in the Underworld: Anonymous Versus Los Zetas in Mexico, 8 Yale J. Int'l Aff. 40, 44 (2013) (describing Brown as "informal spokesperson for Anonymous").

92. See, e.g., Greenwald, supra note 3 (contending "serious journalist" Brown involved himself with online organizations to expose "shadowy and highly secretive underworld of private intelligence and defense contractors").

"investigative journalist" instead of "spokesperson" for the collective.[93] These factors resulted in a perfect-storm scenario that blurred the boundary between journalism and identity fraud in an increasingly online world.

Part II argues that the *Brown* case has drawn attention to shortcomings and ambiguity in the federal identity-fraud statutes that enable potentially unconstitutional restrictions on protected speech. While application of the statute in Brown's case may not result in such restrictions, the broad definitions of § 1028(d) and the lack of an intent requirement in § 1028 enable unconstitutional restrictions in a significant number of cases.[94] Part III then proposes potential solutions for these shortcomings without infringing on the government's aggressive prosecution of malicious identity thieves.

II. IDENTITY FRAUD AND RESTRICTIONS ON PROTECTED SPEECH

Commentary surrounding Barrett Brown's case and mainstream treatment of it has focused on the changing nature of online journalism and potential ramifications for the newsgathering activities of journalists.[95] While it is therefore tempting to argue for a journalist's "right to hyperlink" by relying on the Press Clause of the First Amendment, the Supreme Court has refused to define who qualifies for special privileges as a member of "the press."[96] Due to this lack of precedent, extending

---

93. See Nate Anderson, Prolific "Spokesman" for Anonymous Leaves the Hacker Group, Ars Technica (May 19, 2011, 1:47 PM), http://arstechnica.com/tech-policy/2011/05/why-anonymous-spokesman-is-leaving-the-group/ (on file with the *Columbia Law Review*) (discussing Brown's reasons for distancing himself from Anonymous, including collective's inability to control reckless participants). To further this agenda, Brown arranged an online group to comb through leaked documents and search for evidence of government wrongdoing; he dubbed this initiative "Project PM." See Barrett Brown, The Purpose of Project PM, Barrett Brown (May 29, 2012, 5:39 PM), http://barrettbrown.blogspot.com/2012/05/purpose-of-project-pm.html (on file with the *Columbia Law Review*) (describing purpose of "Project PM" on Brown's personal blog); see also David Carr, A Journalist-Agitator Facing Prison Over a Link, N.Y. Times (Sept. 8, 2013), http://www.nytimes.com/2013/09/09/business/media/a-journalist-agitator-facing-prison-over-a-link.html (on file with the *Columbia Law Review*) (describing "Project PM" as "online collective . . . with a mission of investigating documents unearthed by Anonymous and others"). The IRC to which Brown posted the hyperlink was one such chat room associated with this initiative. See Brown Third Indictment, supra note 5, at 1–2 (detailing contents of hyperlink posted to IRC channel with moniker "#ProjectPM").

94. See infra Part III.A–B (analyzing potential overbreadth and vagueness challenges to §§ 1028 and 1028A and recommending heightened intent requirement).

95. See supra notes 89–93 and accompanying text (summarizing recent commentary regarding Brown's case and presenting viewpoints of several supporters in online articles).

96. Compare Geoffrey R. Stone, Top Secret 38–40 (2007) [hereinafter Stone, Top Secret] (discussing generally understood definition of "journalist" as "member of the 'press'" and difficulty of striking inclusive balance), with Sonja R. West, Press Exceptionalism, 127 Harv. L. Rev. 2434, 2453–62 (2014) [hereinafter West, Press Exceptionalism] (arguing definition of "the press" for purposes of Press Clause of First

special privileges to an online journalist or blogger would require an expansive interpretation of the Press Clause that blurs distinctions between members of the public and "the press."[97]

Part II of this Note instead argues that prosecution for federal identity fraud in connection with sharing a hyperlink to documents containing confidential information may result in unconstitutional restrictions on protected speech under the First Amendment. Part II.A provides a general overview of identity fraud within a First Amendment framework and argues that independent online commentators are particularly vulnerable to identity-fraud prosecution, despite valuable contributions to public discourse. Part II.B discusses two approaches to analyzing potential infringements on protected speech imposed by identity-fraud prosecution. Part II.C then concludes by discussing special problems with dissemination of confidential information unlawfully obtained by third parties.

A. *Identity Fraud and the First Amendment*

The First Amendment protects both "freedom of speech"[98] and freedom "of the press."[99] While this language seems to provide distinct privileges for ordinary citizens and for the *institutional* press, this interpretation is not universally recognized as the original intent of the Founders[100] and has not been explicitly adopted by the Supreme Court.[101] Perhaps for no reason beyond the sheer difficulty of deter-

---

Amendment can and should be limited to workable group and providing several factors upon which such determination may be based).

97. Several scholars have cautioned against this interpretive approach in light of rapid technological change and interconnectivity. See, e.g., West, Press Exceptionalism, supra note 96, at 2445 ("[R]epeat-player specialists with proven track records will do the most valuable work."). But see Adam Cohen, The Media that Need Citizens: The First Amendment and the Fifth Estate, 85 S. Cal. L. Rev. 1, 44–58 (2011) (arguing for First Amendment "right to participate" in mass media and equal treatment of traditional journalists and online journalists or bloggers).

98. U.S. Const. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . .").

99. Id. ("Congress shall make no law . . . abridging the freedom . . . of the press . . . .").

100. See, e.g., Robert H. Bork, Neutral Principles and Some First Amendment Problems, 47 Ind. L.J. 1, 22 (1971) ("The framers seem to have had no coherent theory of free speech and appear not to have been overly concerned with the subject.").

101. Compare Sonja R. West, Awakening the Press Clause, 58 UCLA L. Rev. 1025, 1070 (2011) [hereinafter West, Awakening the Press Clause] (arguing for narrow interpretation of Press Clause and distinguishing institutional press from "an occasional public commentator"), with C. Edwin Baker, The Independent Significance of the Press Clause Under Existing Law, 35 Hofstra L. Rev. 955, 956 (2007) (observing U.S. Supreme Court has largely failed to differentiate between protections afforded by Speech Clause and Press Clause and to define "the press"), and Eugene Volokh, Freedom for the Press as an Industry, or for the Press as a Technology? From the Framing to Today, 160 U. Pa. L. Rev.

mining who is a member of "the press," the Court has largely avoided recognizing unique privileges based on the Press Clause of the First Amendment.[102] Legislatures have proven less hesitant to draw distinctions, though such actions have been mostly to the detriment of the independent commentators at issue here.[103] Several scholars have also attempted to more accurately define the institutional press for purposes of the First Amendment in response to the proliferation of digital content and new media.[104]

This lack of clarity in the Court's First Amendment doctrine presents a practical dilemma: Though many independent commentators exposed to liability for publishing or sharing personal information online would self-identify as journalists or members of "the press," they are unlikely afforded more expansive privileges than those granted to all citizens.[105] Without clearly defined protections under the Court's free-press doctrine, there is a danger that independent commentators may become unique targets for government abuse. Unlike the institutional press, independent commentators are often incapable of exercising substantial influence over a corrupt government or one that stifles dissent.[106] Therefore, while such individuals may fulfill an important role in public dis-

---

459, 461–63 (2012) (arguing original understanding of Press Clause was protection for "press-as-technology," not "press-as-industry").

102. See Branzburg v. Hayes, 408 U.S. 665, 704 (1972) (recognizing unique journalist–source privilege under First Amendment would result in difficult case-by-case determinations of who qualifies for protection); see also Stone, Top Secret, supra note 96, at 38 (discussing difficulty of defining "journalist" for First Amendment purposes and U.S. Supreme Court's reluctance to do so).

103. See, e.g., Free Flow of Information Act of 2013, S. 987, 113th Cong. § 2 (2013) (defining "covered journalist" narrowly to the exclusion of nontraditional entities). For further background on protected entities in proposed federal shield law, compare David Pozen, Why a Media Shield Law May Be a Sieve, Just Security (Oct. 21, 2013, 10:20 AM), http://justsecurity.org/2013/10/21/media-shield-law-sieve-david-pozen/ (on file with the *Columbia Law Review*) (discussing potential weaknesses of proposed federal media shield law), with Sophia Cope, A Federal Shield Law Is Needed to Protect Confidential Sources and the Public's Right to Know: A Reply to David Pozen, Just Security (Oct. 21, 2013, 12:15 PM), http://justsecurity.org/2013/10/21/media-shield-sophia-cope-reply-david-pozen/ (on file with the *Columbia Law Review*) (advocating necessity of media shield law).

104. See, e.g., West, Press Exceptionalism, supra note 96, at 2448–50 (arguing proliferation of online media and digital content does not preempt workable definition of "the press").

105. See supra notes 96–102 and accompanying text (providing overview of widely accepted perspectives on Press Clause and discussing difficulty of defining to whom such privileges should apply); see also West, Awakening the Press Clause, supra note 101, at 1027–33 (arguing Supreme Court has traditionally treated Press Clause as "constitutional redundancy," and advancing independent but narrower definition of "the press" to protect distinct privileges); West, Press Exceptionalism, supra note 96, at 2443–45 (advocating for narrow definition of "the press").

106. See, e.g., Lee C. Bollinger, Uninhibited, Robust, and Wide-Open 109–10 (2010) (arguing "isolated individuals" and "small organizations" cannot "effectively . . . monitor and check the authority of the state").

course comparable even to institutional journalists,[107] they seem exposed to substantial liability without protections rooted elsewhere in the law.

Instead of analyzing implications of the Press Clause, this Note argues that expansive free speech doctrine may justifiably protect independent commentators from identity-fraud charges under §§ 1028 and 1028A.[108] Though independent commentators are vulnerable to liability for identity fraud in ways that institutional journalists are not,[109] existing free speech doctrine may protect public discourse on the Internet without creating an overly broad exception arbitrarily shielding ordinary citizens from liability.

The threshold question in a free speech analysis is whether the relevant statute regulates "speech."[110] Courts have generally distinguished between two categories of restrictions on speech: (1) content-based and (2) content-neutral.[111] Content-based restrictions are those that limit communications based entirely on the message or subject matter of the communication.[112] The Supreme Court has held that content-based restrictions are "presumptively invalid" and courts review them under a rigorous strict scrutiny standard.[113] Content-neutral restrictions, by com-

---

107. See Yochai Benkler, A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate, 46 Harv. C.R.-C.L. L. Rev. 311, 362–63 (2011) [hereinafter Benkler, Free Irresponsible Press] (asserting all organizations and individuals protecting free flow of information of public concern should be entitled to equal protections under First Amendment).

108. See infra Part II.B (exploring potential application of free speech doctrine to identity-fraud statutes).

109. For example, while the *New York Times* may run a scathing editorial in response to government crackdowns on confidential newsgathering, see Editorial, Spying on the Associated Press, N.Y. Times (May 14, 2013), http://www.nytimes.com/2013/05/15/opinion/spying-on-the-associated-press.html (on file with the *Columbia Law Review*) (criticizing Justice Department for searching journalists' phone records in alleged attempt to reveal sources and frighten whistleblowers), an independent blogger arrested on charges of identity fraud is unable to exert anywhere near comparable influence.

110. See Spence v. Washington, 418 U.S. 405, 410–11 (1974) (holding conduct constitutes communicative speech if "intent to convey a particularized message was present, and in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed [or heard] it").

111. See Geoffrey R. Stone, Content-Neutral Restrictions, 54 U. Chi. L. Rev. 46, 46–50 (1987) [hereinafter Stone, Content-Neutral Restrictions] (discussing distinction between content-based and content-neutral restrictions in U.S. Supreme Court jurisprudence). For examples of content-based and content-neutral restrictions, compare Reno v. ACLU, 521 U.S. 844, 870–72 (1997) (holding statute regulating sexually explicit material on Internet constituted content-based restriction on speech), with Ward v. Rock Against Racism, 491 U.S. 781, 803 (1989) (holding ordinance setting sound guidelines content-neutral because objective was generally reducing sound volume and improving concert performances).

112. See Stone, Content-Neutral Restrictions, supra note 111, at 47 (discussing content-based restrictions).

113. See Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 641–43 (1994) (holding content-based restrictions must be subject to "strict scrutiny" review); R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) (holding content-based restrictions "presumptively invalid").

parison, limit speech without regard for the message or subject matter and are evaluated under the more deferential standard of intermediate scrutiny.[114] The Court has also recognized that some statutes not regulating speech may have "incidental" effects on speech.[115] Where an impact on speech is merely incidental, it is generally presumed that a First Amendment issue is not raised.[116] But if that impact is "highly disproportionate" or "significantly limits the opportunities for free expression," the restriction may still be challenged.[117]

The federal identity-fraud statutes are laws of general applicability[118] that prohibit misuse of certain types of confidential personal information. Sections 1028 and 1028A therefore seem to impose only content-neutral restrictions on speech,[119] if not entirely incidental restrictions.[120] While there is a plausible argument that §§ 1028 to 1028A do not impose even incidental restrictions on speech, this seems like an oversimplification of the prohibited conduct and the nature of confidential personal information itself. Part II.B attempts to define those circumstances in which identity-fraud statutes impose restrictions on protected speech.

---

114. See *Turner Broad. Sys.*, 512 U.S. at 642 (holding content-neutral regulations trigger intermediate scrutiny); Stone, Content-Neutral Restrictions, supra note 111, at 48–50 (explaining muddled standard of intermediate scrutiny for content-neutral restrictions).

115. See Stone, Top Secret, supra note 96, at 30–33 (summarizing incidental-effects doctrine and three categories of free speech restrictions); see also Elena Kagan, Private Speech, Public Purpose: The Role of Governmental Motive in First Amendment Doctrine, 63 U. Chi. L. Rev. 413, 494–508 (1996) (distinguishing between "direct" and "incidental" effects by focusing on impermissible government motives).

116. See United States v. O'Brien, 391 U.S. 367, 377 (1968) (holding incidental restrictions on speech are justified where they are no greater than necessary to further substantial government interest unrelated to suppression of free expression).

117. Stone, Content-Neutral Restrictions, supra note 111, at 114.

118. See Cohen v. Cowles Media Co., 501 U.S. 663, 670 (1991) (holding Minnesota law generally applicable because "daily transactions of all the citizens" were affected, as opposed to targeted effects on press); cf. Emp't Div. v. Smith, 494 U.S. 872, 879 (1990) (holding incidental effects on free exercise rights under First Amendment do not warrant invalidation of neutral law of general applicability). For further discussion of neutrality in constitutional law, see generally Cass R. Sunstein, Neutrality in Constitutional Law, 92 Colum. L. Rev. 1 (1992) (exploring concept of neutrality in constitutional law premised on existing distributions as baseline measurement).

119. While some may argue that restrictions on the transfer of confidential information are, in fact, content-based restrictions, this argument is not viable. Even if confidential personal information has expressive value, §§ 1028 and 1028A do not target the message conveyed by transferring such information. See supra notes 110–114 and accompanying text (distinguishing content-based and content-neutral restrictions).

120. See Stone, Content-Neutral Restrictions, supra note 111, at 48 (observing content-neutral restrictions "limit expression without regard to the content or communicative impact of the message conveyed").

B. *Protecting Speech in the Identity-Fraud Context*

First Amendment challenges to the federal identity-fraud statutes may be viable in several scenarios, though sharing information via hyperlink poses particularly unique challenges. These challenges stem from two observations. First, the Internet has evolved into a uniquely valuable medium of communication with hyperlinking as a fundamental component.[121] Second, the complex dynamics of hacktivist campaigns and confidential-document dumps have resulted in many nonmalicious individuals accessing or sharing confidential information via hyperlink.[122] Part II.B responds to these concerns by addressing the identity-fraud statutes generally and then devoting particular attention to the context of hyperlinking.[123] Part II.B.1 analyzes potential First Amendment challenges by focusing on the actual information regulated—the "means of identification" and "authentication features"—while Part II.B.2 conducts the same analysis focusing on the hyperlink itself as potentially protected speech.

1. *Identity-Fraud Statutes as Restrictions on Protected Speech.* — Sections 1028 and 1028A prohibit the unlawful transfer, production, possession, or use of "means of identification"[124] and "authentication features."[125] Analyzing potential First Amendment challenges by focusing on the confidential personal information accessed or shared results in two relevant First Amendment questions: whether "means of identification," "authentication features," or the underlying documents in which those two categories of features exist can *ever* constitute speech, and, if so, whether §§ 1028 and 1028A regulate speech or nonspeech elements.[126] If

---

121. For a more comprehensive argument on the democratizing and liberating effects of the Internet, see generally Yochai Benkler, Wealth of Networks (2010) [hereinafter Benkler, Wealth of Networks].

122. See supra Part I.C (discussing modern dynamics of hacktivist campaigns and observing actors other than those involved in cyberattacks are often drawn to information released).

123. See supra notes 98–114 and accompanying text (discussing briefly two analytical approaches courts may take in responding to First Amendment challenges to identity-fraud statutes).

124. 18 U.S.C. § 1028A(a)(1) (2012).

125. Id. § 1028(a)(2).

126. See United States v. Playboy Entm't Grp., Inc., 529 U.S. 803, 813 (2000) (analyzing content-based restriction under strict scrutiny framework where statute merely restricted sexual speech); Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 643 (1994) (discussing distinction on basis of whether ideas or subject matter is regulated and providing two-tier framework for review); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 453–54 (2d Cir. 2001) (finding, where target of regulation contains both speech and nonspeech components, courts should identify which component is being targeted and tailor degree of scrutiny accordingly); Stone, Content-Neutral Restrictions, supra note 111, at 47–48 (discussing content-based and content-neutral distinction). But see City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 47–48 (1986) (holding even facially content-based regulation may be treated as content-neutral if regulation is motivated by permissible content-neutral purpose).

courts scrutinize the actual hyperlink in this analysis, the First Amendment challenge becomes more complicated and likely turns on the role of the hyperlink in a particular factual scenario.[127]

"Means of identification"—such as credit card numbers and email addresses—undoubtedly serve functional or nonspeech roles.[128] The function of a "means of identification" or identification document is somewhat self-explanatory: Entities use them to identify a specific individual and grant access, manage finances, or otherwise link that individual with their online and offline lives.[129] Though it is true that a name or number[130] may be communicative, names and numbers without more do not always communicate a *message*.[131] Furthermore, it seems even less likely that an "authentication feature"[132] would communicate a message protected by the First Amendment, since the sole function of such a feature is to verify the authenticity of another document, string of characters, or document-making implement.[133]

It is a fundamental principle of First Amendment doctrine that the right to free speech is not absolute and that certain categories of speech may be justifiably prohibited or regulated by the government,[134] such as

127. For example, where a hyperlink is used in parody, criticism, or political speech, the potential First Amendment challenges appear to be much stronger than in a scenario whereby a hyperlink is used solely for file sharing or access. See infra notes 155–161 and accompanying text (discussing hyperlink analysis in context of trademark infringement and "commercial use").

128. See, e.g., Credit Card Definition, Oxford Dictionaries, http://www.oxforddictionaries.com/us/definition/american_english/credit-card?q=credit+card (on file with the *Columbia Law Review*) (last visited Mar. 5, 2015) (defining "credit card" purpose as mechanism "to purchase goods or services on credit").

129. See 18 U.S.C. § 1028(d)(7) (defining "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual").

130. Id.

131. See Stone, Content-Neutral Restrictions, supra note 111, at 47–51, 105–08 (observing lack of *communicative message* is relevant to determining degree of First Amendment scrutiny).

132. 18 U.S.C. §1028(d)(1) (defining "authentication feature" as "any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature").

133. See, e.g., United States v. Baker, 435 F. App'x 2, 4 (D.C. Cir. 2011) (observing purpose of imprinting hologram on state driver's license is to identify license as genuine state-issued document); United States v. Rodriguez-Cisneros, 916 F. Supp. 2d 932, 935 (D. Neb. 2013) (holding purpose of "authentication feature" is to determine whether identification document is "counterfeit, altered, or otherwise falsified").

134. See Chaplinsky v. New Hampshire, 315 U.S. 568, 570–72 (1942) (discussing categories of speech entitled to limited protection under First Amendment); Schenck v. United States, 249 U.S. 47, 52 (1919) (discussing qualified right to free speech and providing "clear and present danger" test).

obscenity,[135] "fighting words,"[136] and incitement of illegal activity.[137] Some categories of speech, however, such as political[138] or religious speech,[139] represent the strongest examples of protected speech under the First Amendment. In certain limited contexts, there is a plausible argument that these names or numbers are essential to a message communicated by documents in which "means of identification" or "authentication features" exist.[140] Therefore, where personally identifiable information constitutes merely one component of a larger message—as will often be the case with massive dumps of confidential information carried out for political purposes—courts must determine whether the value of the speech outweighs the potential damage of disseminating personal information in a specific context.[141]

Imagine a writer at the *New York Times* stumbles across an extensive list, anonymously posted to WikiLeaks, of individuals subject to federal background investigations and personal information, such as home addresses, phone numbers, and online usernames.[142] Some entries ap-

---

135. See, e.g., Miller v. California, 413 U.S. 15, 24, 36 (1973) (holding obscene speech unprotected under First Amendment and providing balancing test to determine whether speech is obscene).

136. See, e.g. *Chaplinsky*, 315 U.S. at 571–72 (holding insulting or fighting words whose "very utterance inflict injury" unprotected under First Amendment).

137. See, e.g., Brandenburg v. Ohio, 395 U.S. 444, 447–48 (1969) (holding state may not curtail speech advocating use of force or violation of law except where such advocacy is directed towards and likely to incite "imminent lawless action").

138. See Buckley v. Valeo, 424 U.S. 1, 14 (1976) (observing political speech and expression entitled to substantial protection under First Amendment); see also Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 365 (2010) (reaffirming *Buckley* and holding First Amendment protects corporation's freedom of speech).

139. See, e.g., Widmar v. Vincent, 454 U.S. 263, 277 (1981) (holding First Amendment protected religious speech where public university created open forum for student expression).

140. Indeed, this seems to be the argument that Barrett Brown's defense team and his supporters made in the context of the Stratfor document leak. See, e.g., Statement from Barrett Brown, "Hooray for the Justice Department," Pastebin (Apr. 24, 2012), http://pastebin.com/h93tpbtD (on file with the *Columbia Law Review*) (discussing Brown's suspicions regarding inappropriate government ties with Stratfor Global Intelligence, HBGary Federal, and other third parties).

141. It seems likely that most such scenarios will fall under the category of "political speech," as appears to be the case in *United States v. Brown*. Even so, the policy objectives underpinning federal identity-fraud statutes will weigh heavily in the court's analysis since §§ 1028 and 1028A appear to be content-neutral regulations at most. See supra notes 111–117 and accompanying text (outlining distinction between content-based and content-neutral restrictions in free speech analysis).

142. This hypothetical was adapted from recent revelations regarding the security firm U.S. Investigations Services (USIS). There is no evidence that this sequence of events actually took place, but it provides an interesting vehicle for analysis. See Matt Apuzzo, Security Check Firm Said to Have Defrauded U.S., N.Y. Times (Jan. 23, 2014), http://www.nytimes.com/2014/01/23/us/security-check-firm-said-to-have-defrauded-us.html (on file with the *Columbia Law Review*) (highlighting Justice Department allegation that USIS fraudulently submitted 650,000 uncompleted security checks).

pear legitimate, but the writer also notices thousands are bogus. Believing the list of investigated individuals provides evidence of unsecure practices and government waste, the writer shares a hyperlink to these documents with her editorial team at the *Times*, along with a message expressing interest in writing a related story. While most would recognize this conduct as a legitimate exercise of protected speech, the writer appears to have transferred thousands of "means of identification," committing identity fraud and exposing several individuals to criminal liability in the process.[143]

2. *Hyperlinking Prohibitions as Restrictions on Protected Speech.* — Hyperlinking as a means of sharing access to confidential personal information warrants special attention due to hyperlinking's importance as a medium of digital communication.[144] Hyperlinks generally consist of both expressive and non-expressive elements.[145] Though used to connect different locations on the Internet and pages on a single website, hyperlinks may also serve as a sign of authority or affiliation.[146] Links may be used by the general public to facilitate access to obscure information, draw mainstream attention to a particular issue, or even to make political statements by manipulating connections between webpages.[147] While the expressive elements of hyperlinks may be directly regulated in contexts such as trademark infringement under the Lanham Act,[148] prohibitions on conduct related to identity fraud only incidentally restrict the expressive elements of hyperlinking.[149]

Turning to hyperlinks within the scope of §§ 1028 and 1028A, the question becomes whether sharing a hyperlink to documents containing confidential personal information can constitute protected speech.[150]

---

143. This outcome assumes the court is using the government's interpretation of "transferring" initially asserted in *United States v. Brown*. See supra notes 4–7 and accompanying text (discussing charges against Brown and prosecutor's interpretation of "transfer").

144. Hyperlinking may prove particularly relevant in the circumstances of "massive dumps," as discussed in Part I.C above, due to the impracticality of sharing large amounts of information via alternative means.

145. See Anjali Dalal, Protecting Hyperlinks and Preserving First Amendment Values on the Internet, 13 U. Pa. J. Const. L. 1017, 1024–39 (2011) (discussing both functional and expressive elements of hyperlinks).

146. See id. at 1037–40 (explaining role of hyperlink as "signal of credibility").

147. See id. at 1036–37 (discussing "Googlebombing" of President George W. Bush and democratic nature of hyperlinking to information on Internet).

148. See infra notes 158–164 and accompanying text (discussing hyperlinking and trademark infringement under Lanham Act).

149. See supra notes 111–117 and accompanying text (discussing content-neutral restrictions on speech and distinguishing between "direct" and "incidental" effects).

150. See Spence v. Washington, 418 U.S. 405, 410–15 (1974) (holding context in which symbol is used relevant to determining whether conduct is expressive and protected by First Amendment). In *Spence*, the Court emphasized two factors relevant to determining whether regulated conduct is itself communicative: (1) "intent to convey a particularized

The Supreme Court has noted "[i]t is possible to find some kernel of expression in almost every activity a person undertakes," but that such a minimal degree of expression is insufficient to grant First Amendment protection to the conduct at issue.[151] However, whether hyperlinking to unlawfully obtained "means of identification" or "authentication features"[152] actually constitutes protected speech for purposes of the First Amendment represents a narrow question on which there is limited case law directly on point.

Several related developments in the area of intellectual property may prove informative for the identity-fraud context because they provide detailed legal and technical analysis of hyperlinks. In *Pearson Education, Inc. v. Ishayev*, a federal district court determined that emailing a hyperlink to copyrighted works did not constitute "distribut[ing] copies"[153] in violation of an owner's exclusive rights.[154] Drawing on precedent in the Southern District of New York and Ninth Circuit,[155] the court explained that sharing a hyperlink does not constitute copyright infringement because a hyperlink is "the digital equivalent of giving the recipient driving directions to another website on the Internet."[156] In other words, the hyperlink itself does not contain substantive content; it merely contains HTML instructions directing the recipient to the content's location on the Internet.[157]

Several circuit courts have also reviewed hyperlinking in the context of "commercial use" of trademarks under the Lanham Act.[158] While these cases have dealt with varied factual scenarios, courts consider the totality of the circumstances to determine whether hyperlinking to trademarked materials constitutes commercial use.[159] As part of this analysis,

---

message" and (2) whether "in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it." Id. at 410–11.

151. City of Dallas v. Stanglin, 490 U.S. 19, 25 (1989).

152. 18 U.S.C. § 1028(d) (2012) (providing statutory definitions of relevant terms).

153. 17 U.S.C. § 106(3) (2012).

154. Pearson Educ. v. Ishayev, 963 F. Supp. 2d 239, 250–51 (S.D.N.Y. 2013).

155. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1161 (9th Cir. 2007) (holding HTML instructions rerouting users to infringing image insufficient to demonstrate copyright infringement); MyPlayCity, Inc. v. Conduit Ltd., No. 10 CIV. 1615 CM, 2012 WL 1107648 (S.D.N.Y. Mar. 30, 2012) (holding actual transfer of files must occur for direct liability to attach), aff'd, No. 10 CIV. 1615 CM, 2012 WL 2929392 (S.D.N.Y. July 18, 2012); Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660(SHS), 2002 WL 1997918, at *4 (S.D.N.Y. Aug. 29, 2002) (holding dissemination of hyperlinks to infringing files insufficient to constitute infringement).

156. *Pearson Educ.*, 963 F. Supp. 2d at 250–51.

157. Id.; see also *Perfect 10*, 508 F.3d at 1161 ("Providing . . . HTML instructions is not equivalent to showing a copy."); *MyPlayCity*, 2012 WL 1107648, at *12 (holding hyperlinking insufficient to establish direct infringement of exclusive distribution right).

158. 15 U.S.C. § 1125 (2012).

159. See Utah Lighthouse Ministry v. Found. for Apologetic Info. & Research, 527 F.3d 1045, 1052 (10th Cir. 2008) (holding hyperlink to trademarked domain name not "commercial use" in context of parody without any further indication of commercial

courts look to the underlying purpose of the Lanham Act—protecting the ability of consumers to distinguish between competitors—to determine whether or not hyperlinking constitutes "commercial use."[160] Courts have also considered whether imposition of liability would unnecessarily infringe on an individual's First Amendment rights, though the factual circumstances in those cases greatly differ.[161] This judicial approach recognizes hyperlinks are multifunctional objects that must be analyzed in both their online context and the context of the statutory prohibition.[162]

Despite an understanding of hyperlinks as "HTML instructions" that do not necessarily violate a copyright owner's exclusive right to distribute[163] or result in commercial use problems under the Lanham Act, several cases brought under the anticircumvention provision of the Digital Millennium Copyright Act (DMCA)[164] have resulted in liability for the mere posting of hyperlinks. In *Universal City Studios v. Reimerdes*, a federal district court determined that posting hyperlinks to decryption software on a website constituted "offering, providing, or otherwise trafficking in" prohibited software.[165] According to the trial court, making the hyperlinks publicly available on a website was "the functional equivalent of transferring the [decryption software] code to the user themselves."[166] Beyond the statutory issues, the trial court was asked to address

---

activities); Bosley Med. Inst., Inc. v. Kremer, 403 F.3d 672, 679–80 (9th Cir. 2005) (finding trademark use noncommercial because use did not mislead consumers); Taubman Co. v. Webfeats, 319 F.3d 770, 775 (6th Cir. 2003) (finding presence of even two commercial links potentially sufficient to establish "commercial use" under Lanham Act); People for Ethical Treatment of Animals (PETA) v. Doughney, 263 F.3d 359, 367 (4th Cir. 2001) (holding thirty commercial links sufficient to make use of trademarked domain name "commercial use").

160. See, e.g., *Utah Lighthouse Ministry*, 527 F.3d at 1053 (observing, where limited number of hyperlinks on webpage link to noncommercial pages of another site, Lanham Act policy of consumer protection is not implicated); *Bosley Med. Inst.*, 403 F.3d at 676–80 (finding defendant's use of mark does not stifle consumer ability to distinguish between competing products and thus does not implicate underlying purpose of Lanham Act).

161. See, e.g., *PETA*, 263 F.3d at 370 (discussing First Amendment right to self-expression in form of parody website); *Bosley Med. Inst.*, 403 F.3d at 682 (discussing domain names and source identifiers in First Amendment context).

162. This Note does not purport to offer an exhaustive investigation of the technical, legal, or social nature of hyperlinks. For more background on hyperlinks and the many roles that they fulfill, see generally Dalal, supra note 145, at 1017 (discussing nature of hyperlinks in great depth and arguing hyperlinks are both medium and message).

163. 17 U.S.C. § 106(3) (2012) (proving exclusive right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending").

164. 17 U.S.C. § 1201(a)(2) (prohibiting "offer[ing] to the public, provid[ing], or otherwise traffic[king]" in decryption technology, as defined by DMCA).

165. Universal City Studios v. Reimerdes (*Universal I*), 111 F. Supp. 2d 294, 341 (S.D.N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

166. Id. at 325.

several constitutional challenges—including an argument that the anti-circumvention provision of the DMCA violates the First Amendment—but ultimately determined that the DMCA survived all constitutional challenges.[167]

Applying the requirements pertaining to content-neutral regulations as laid out in *O'Brien*,[168] *Turner Broadcasting*,[169] and *Ward*,[170] the trial court determined that the anticircumvention provision of the DMCA did not constitute unlawful infringement of protected speech because it protected a substantial government interest without unnecessarily infringing on free expression.[171] While *Universal I* was affirmed on appeal, the Second Circuit explicitly reaffirmed the First Amendment holding below without adopting the trial court's more rigorous analysis.[172] According to the circuit court, since computer code contains both speech and non-speech elements, the level of scrutiny applied should depend on the elements targeted by a particular regulation; since the anticircumvention provision of the DMCA did not target the expressive elements of decryption software, it was treated as a content-neutral regulation subject to intermediate scrutiny.[173]

Drawing on these three lines of doctrine, it is unclear which is most analogous to identity fraud under § 1028(a)(2). The statutory language provides that it is unlawful for any person to "knowingly transfer[] an . . . authentication feature."[174] It is true that a hyperlink to unlawfully obtained authentication features appears to do no more than the set of "HTML instructions" in copyright infringement cases like *Pearson Education* or *Perfect 10*, but it is unclear whether "means of identification"

---

167. The defendants in *Universal I* raised two First Amendment challenges, arguing (1) the decryption software prohibited by the DMCA was protected speech, and (2) the DMCA's prohibition on distribution of decryption software is unconstitutionally broad because it prevents fair use of software and, therefore, prohibiting linking to software on a website is also an unconstitutionally overbroad prohibition. Id. at 325–26.

168. United States v. O'Brien, 391 U.S. 367, 377 (1968) (holding incidental restrictions on speech are justified where no greater than necessary to further substantial government interest unrelated to suppression of free expression).

169. Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642–43 (1994) (holding content-based restrictions on speech must be subject to strict scrutiny review).

170. Ward v. Rock Against Racism, 491 U.S. 781, 798–99 (1989) (holding restriction "narrowly tailored" to government's content-neutral interest if not overbroad, even if less-restrictive means are available).

171. *Universal I*, 111 F. Supp. 2d at 339–41; see also United States v. Elcom, 203 F. Supp. 2d 1111, 1128 (N.D. Cal. 2002) (observing lack of evidence indicating congressional intent to restrict freedom of expression).

172. See Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443–35, 459–60 (2d Cir. 2001) (affirming trial court decision to enjoin website from making hyperlinks to decryption software available on website).

173. See id. at 450–51, 454–55 (determining DMCA's anticircumvention provision is content-neutral regulation and thus subject only to intermediate scrutiny under First Amendment analysis).

174. 18 U.S.C. § 1028(a)(2) (2012).

and "authentication features" are more analogous to copyrighted works or the harm caused by disseminating the location of those works.[175] More interesting is the question of whether the framework applied in *Corley* would also be applicable in the identity-fraud context. It is unlikely that credit card numbers or any other "means of identification" or "authentication features" could constitute computer code similar to the decryption software at issue in *Corley*. It is certainly possible, however, that "authentication features" or "means of identification" may sometimes contain both expressive and functional elements.[176]

If courts adopt an interpretive approach similar to *Corley*, they must first determine whether the expressive or non-expressive elements of the features are being restricted and then subject the restriction to the appropriate standard of review.[177] As discussed in Parts II.B.1 and II.B.2, however, it is unclear whether courts should look toward the information regulated—"means of identification" and "authentication features"—or the hyperlink used to share the location of that information.[178] Where a hyperlink to nothing more than a list of credit card numbers is shared,[179] it would be difficult to argue that protected speech is restricted by an identity-fraud prosecution.[180] But where many fewer credit card numbers are included in a dump of several million documents demonstrating alleged government wrongdoing,[181] as alleged in the *Brown* case,[182] the

175. For example, the *Perfect 10* Court's emphasis on imposing liability for distribution of actual copies seems responsive to the harm of market dilution that copyright law seeks to address. See Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007) (affirming district court's rejection of distribution-infringement claim because "Google did not communicate the full-size images to the user's computer"). For an exhaustive analysis of the distribution right in copyright law, see generally Peter S. Menell, In Search of Copyright's Lost Ark: Interpreting the Right to Distribute in the Internet Age, 59 J. Copyright Soc'y U.S.A. 1, 5–6 (2011) (analyzing purpose and history of exclusive right of distribution in U.S. copyright law).

176. According to the *Corley* court, where the target of a regulation has both expressive and non-expressive elements, the key is determining which component is being targeted. This dilemma is partly what makes computer code unique in the First Amendment context; since computer code almost always requires a degree of human interaction or expression, prohibitions on the expressive elements will be seen as content-based regulations, whereas regulations of non-expressive elements will be seen as content-neutral regulations. See *Corley*, 273 F.3d at 453–54.

177. See supra notes 172–173 and accompanying text (discussing Second Circuit's analysis of expressive and non-expressive elements in *Corley*).

178. See supra Part II.B (discussing two interpretive approaches courts may take when analyzing First Amendment challenges to federal identity-fraud statutes).

179. See, e.g., United States v. Giannone, 360 F. App'x 473, 476–77 (4th Cir. 2010) (discussing transmission of debit card numbers and accountholder names for purpose of committing identity fraud).

180. Cf. Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (prohibiting speech that encourages "imminent lawless action").

181. WikiLeaks claims over five million emails were taken from Stratfor systems and leaked on the Internet, see The Global Intelligence Files, WikiLeaks, http://wikileaks.org/the-gifiles.html (on file with the *Columbia Law Review*) (last visited Jan. 24, 2015), though

argument becomes more viable. Defendants in such circumstances may argue either that they either did not know the information was available at the hyperlinked location[183] or that the information was itself necessary to the message the documents conveyed.[184]

3. Standard of Review for Hyperlinking Restrictions. — When reviewing content-neutral restrictions on speech, courts generally apply one of three standards of scrutiny; the court's choice depends on the degree to which valued speech is restricted and the significance of the government interest involved.[185] The standard of "intermediate scrutiny" is ordinarily invoked when reviewing content-neutral restrictions; it requires that courts ask only whether a content-neutral restriction is "narrowly tailored to serve a significant governmental interest."[186] However, Geoffrey Stone has argued that courts may apply the heightened standard of strict scrutiny (or a more rigorous form of intermediate scrutiny) to a content-neutral restriction on speech in certain circumstances. This would require the government to demonstrate a "compelling interest" instead of a merely "substantial interest."[187]

Some scholars have argued hyperlinking prohibitions are one such scenario necessitating heightened scrutiny—even in the context of content-neutral restrictions—due to the unique value hyperlinks provide

---

five thousand credit card numbers were included in those documents and Brown was charged with trafficking in twelve "means of identification," see Brown Third Indictment, supra note 5, at 4–5 (enumerating identity-fraud charges).

182. See supra notes 81–93 and accompanying text (discussing factual circumstances of Brown's case and Stratfor Global Intelligence leak).

183. 18 U.S.C. §§ 1028–1028A (2012) (requiring defendant "knowingly" traffic in prohibited information). Admittedly, this issue may be resolved by requirements of the "beyond a reasonable doubt" standard. See In re Winship, 397 U.S. 358, 364 (1970) (holding "Due Process Clause protects the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged").

184. See supra notes 134–141 and accompanying text (discussing potential argument for political speech). For further discussion on the political-speech doctrine, see Buckley v. Valeo, 424 U.S. 1, 14 (1976) (observing political speech and expression entitled to substantial protection under First Amendment).

185. See Stone, Content-Neutral Restrictions, supra note 111, at 50–54 (observing courts apply three standards of scrutiny in analyzing content-neutral restrictions). Stone also argues courts may find content-neutral restrictions unconstitutional as to one speaker if effects are disproportionate to the government interest protected but not as to a speaker upon whom the effects are modest. Id. at 63; see also N.Y. Times Co. v. Sullivan, 376 U.S. 254, 285 (1964) (asserting, in cases "where [a] line must be drawn," the Court should examine whether restrictions on speech violate principles of First and Fourteenth Amendments).

186. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

187. See Stone, Content-Neutral Restrictions, supra note 111, at 50 (quoting Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)); see also *Globe Newspaper*, 457 U.S. at 607–09 (holding government's compelling interest in limiting public attendance at sex-crime trials involving minors did not outweigh potential First Amendment infringements of mandatory closure rules).

to online communication. Expanding on Stone's three-step formulation of content-neutral review, Anjali Dalal argues that the content-neutral doctrine is essentially an "effects-based doctrine" in which courts evaluate the "net effect on valued speech."[188] Since hyperlinking is essential to uniquely valuable online communication, restrictions on hyperlinking where First Amendment rights are implicated should be subject to a heightened standard of review.[189] In making this argument, Dalal relies heavily on the seminal case *New York Times Co. v. Sullivan*[190] and highlights the Internet as a medium of communication rivaling the importance of newspapers in the 1960s.[191] This analytical approach is discussed further in Part III.B.

C. *Disseminating Information Unlawfully Obtained*

Part I.C of this Note highlighted increasingly complex and anonymous interactions between individuals who (1) infiltrate private computer systems and release confidential information, (2) exploit confidential personal information released on the Internet, and (3) access or share dumped confidential information for nonmalicious purposes. Parts II.A and II.B explored several concerns regarding unconstitutional restrictions on protected speech resulting from prosecution for identity fraud. Part II.C argues that recent developments in the Supreme Court's First Amendment doctrine highlight the disconcerting impact of imposing criminal liability on those who access and share confidential information unlawfully obtained by third parties.[192]

1. Private Information Unlawfully Obtained. — In *Bartnicki v. Vopper*,[193] the Court addressed a factual scenario similar to that in *United States v. Brown*,[194] though the medium of communication was different: A local

188. Dalal, supra note 145, at 1049.

189. Id. at 1068–72 (arguing Court should adopt less deferential standard of review where statutory restrictions inhibit communicative value of hyperlinking on Internet). It is valuable to note, however, that Dalal does not see this approach as allowing the encouragement of illegality. Id. at 1069.

190. 376 U.S. 254.

191. See Dalal, supra note 145, at 1068–72 (discussing intent-based approach of *Sullivan* and importance of print newspapers to public discourse at time *Sullivan* was decided). For further discussion on the unique value of hyperlinking and the Internet to public discourse, see infra notes 216–217 and accompanying text (discussing need to protect any individual who facilitates free flow of information that is matter of public concern).

192. Where information is disseminated on the Internet because of a hacktivist campaign, information will almost certainly be unlawfully obtained by individuals responsible for infiltrating private data systems. See supra Part I.C.2 (discussing hacktivist dynamics and applicability of CFAA to various degrees of involvement in hacktivist campaigns).

193. 532 U.S. 514 (2001).

194. See supra notes 78–93 and accompanying text (discussing Brown's receipt of information unlawfully obtained by third parties and subsequent sharing of information via hyperlink).

radio personality received information from a third party who had obtained that information unlawfully.[195] The radio personality then disseminated the information to the public by means of his radio program.[196] Though *Bartnicki* recognized that unlawfully intercepting a private phone conversation implicates significant individual privacy rights,[197] it determined the radio personality could not be held liable because he had not himself unlawfully obtained the information. Under these circumstances, disclosure of information in the public interest outweighed individual privacy rights.[198]

While *Bartnicki* establishes that unlawful interception of information by a third party does not automatically limit the First Amendment right to publish, it does little to define the boundaries of "public concern."[199] Examining the line of cases that *Bartnicki* builds upon, the concept of "public concern" may clearly be stretched further than anticipated; it has been used to justify publication of classified documents concerning the Vietnam War,[200] names of juvenile defendants in criminal proceedings,[201] names of alleged rape victims,[202] and confidential inquiries before a state agency.[203] While one may argue that personally identifiable information

---

195. See supra notes 78–93 and accompanying text (discussing Brown's liability for distribution of unlawfully obtained information).

196. See *Bartnicki*, 532 U.S. at 518–19, 534–35 (holding recorded individuals' rights to conversational privacy did not outweigh public interest in disclosure of information contained in conversation unlawfully obtained by third party).

197. Id. at 532–33 (discussing importance of conversational privacy right and judicial need to avoid chilling effects on private conversations).

198. Id. The Court's holding in *Bartnicki* appears to be unusually broad. But Justice Breyer's concurrence tempered *Bartnicki*'s breadth by stressing the narrowness of its application and the threat of imminent physical injury contained in the recording as a matter of unusually strong public concern. Id. at 535–36 (Breyer, J., concurring).

199. See id. at 533–34 (majority opinion) ("The enforcement of [the specific statutory provision at issue] . . . implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern."). The breadth of the decision and reliance on undefined boundaries of "public concern" seemed to at least partially inform the *Bartnicki* dissent. See id. at 555–56 (Rehnquist, C.J., dissenting) (arguing standard of "public concern" should not overcome individual right to conversational privacy).

200. See, e.g., N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (holding prior restraints on publication of matters in public interest presumptively unconstitutional).

201. See, e.g., Smith v. Daily Mail Pub'g Co., 443 U.S. 97, 101–02 (1979) (holding publication of "lawfully obtained, truthful information" about juvenile defendant should not be enjoined).

202. See, e.g., Fla. Star v. B.J.F., 491 U.S. 524, 532 (1989) (holding publication of alleged rape victim's name should not be enjoined when obtained lawfully from public records).

203. See, e.g., Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829, 837 (1978) (holding publication of confidential proceedings of state body should not be enjoined). The line of cases in notes 200–203 are generally referred to as the *Daily Mail* principle or doctrine. See Richard D. Shoop, Note, *Bartnicki v. Vopper*, 17 Berkeley Tech. L.J. 449, 454–56 (2002) (discussing *Daily Mail* principle and line of cases).

such as credit card numbers should be excluded from this well-established exception for matters of "public concern," at least one court has held that even social security numbers may be posted on the Internet by private citizens when those numbers are *lawfully* obtained from public records previously available on government websites and displayed in their original form.[204] According to the Fourth Circuit in *Ostergren v. Cuccinelli*, the government's decision to make information publicly available itself implies the information is a matter of public concern.[205]

2. Knowledge of Unlawfulness. — Two important questions remain open following *Bartnicki* and are particularly relevant in the context of information anonymously posted on the Internet. The first is whether *Bartnicki* applies to circumstances in which an individual *knows* the information received was unlawfully obtained.[206] Though the radio personality in *Bartnicki* broadcast an unlawfully obtained conversation on his show, it is unclear whether he knew the conversation was illegally intercepted.[207] Without judicial clarification in the identity-fraud context, the government would need to prove no more than knowledge the information belonged to another person and was contained in documents transmitted.[208] This question seems at least slightly more complicated when dealing with aggravated identity theft because the Court has held that an individual must knowingly transfer a means of identification that they also know *belongs* to another person.[209] In other words, even if an individual knows the information received and shared contains "means of identification," that individual must also know the "means of identification" belong to another person to be convicted under § 1028A.[210]

---

204. See Ostergren v. Cuccinelli, 615 F.3d 263, 272 (4th Cir. 2010) (holding prohibiting publication of unredacted social security numbers infringed privacy activist's First Amendment rights where unredacted numbers were published in form of full government documents previously available on Internet).

205. Id. at 276 ("Public records by their very nature are of interest to those concerned with the administration of government." (citing Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975)).

206. See William E. Lee, Probing Secrets: The Press and Inchoate Liability for Newsgathering Crimes, 36 Am. J. Crim. L. 129, 147–48 (2009) (discussing ambiguity concerning knowledge of unlawful interception in wake of *Bartnicki*).

207. See Bartnicki v. Vopper, 532 U.S. 514, 517–18 (2001) (noting radio personality may not have had actual knowledge that interception was unlawful).

208. See Rodney A. Smolla, Information as Contraband: The First Amendment and Liability for Trafficking in Speech, 96 Nw. U. L. Rev. 1099, 1148–49 (2002) (distinguishing antitrafficking statutes from statute at issue in Fla. Star v. B.J.F., 491 U.S. 524, 532 (1989), by highlighting presence of scienter requirement).

209. See Flores-Figueroa v. United States, 556 U.S. 646, 647 (2009) (holding defendant could not be convicted for aggravated identity theft without government demonstrating defendant knew means of identification belonged to another person, as opposed to being merely counterfeit).

210. Id.

The second important question for purposes of this Note is whether *Bartnicki* also extends to ordinary citizens, as opposed to media personalities and institutional journalists. Though *Ostergren* held that social security numbers may be published by an independent commentator when *lawfully* obtained from public records, the Fourth Circuit did not address whether publication would be allowed if the numbers had been *unlawfully* obtained by a third party.[211] Recent cases such as *United States v. Brown*[212] and *United States v. Auernheimer*[213] further call into question the applicability of *Bartnicki* to independent commentators and ordinary citizens. While related decisions such as *United States v. Stevens* recognize that speech derivative to third-party illegality may sometimes be protected under the First Amendment,[214] these decisions address more traditional forms of speech and are therefore only partly analogous.[215]

Many scholars assert the Internet and increased accessibility of information can serve important democratic functions unfulfillable via the institutional press.[216] These arguments tend to support equal treatment of any individual publishing in the public interest and furthering

---

211. See Ostergren v. Cuccinelli, 615 F.3d 263, 272 (4th Cir. 2010) (emphasizing public availability of numbers and publication of numbers in original, publicly available format). Lower courts have also refused to interpret *Bartnicki* as granting a First Amendment right of disclosure to anyone who lawfully obtains information, particularly where the recipient is under a contractual or otherwise special obligation to keep the information confidential. See, e.g., Boehner v. McDermott, 484 F.3d 573, 577–78 (D.C. Cir. 2007) (holding member of House Ethics Committee did not have First Amendment right to disclose recording received while exercising responsibilities as member of committee).

212. See supra notes 1–13, 78–81 (discussing factual background and numerous identity-fraud charges against Barrett Brown).

213. Privacy experts filed an amicus brief in the *Auernheimer* appeal to express concern about unforeseen implications of a decision finding Auernheimer guilty under the CFAA for incrementing the URL of a public website and publicly exposing information gained through that process. See Brief of Amici Curiae Mozilla Foundation, Computer Scientists, Security and Privacy Experts in Support of Defendant-Appellant and Reversal at 7–8, United States v. Auernheimer, 748 F.3d 525 (3d Cir. Apr. 11, 2014) (No. 13-1816).

214. 130 S. Ct. 1577, 1584, 1592 (2010) (holding federal statute was presumptively invalid content-based restriction and unconstitutionally overbroad restriction on protected speech).

215. Id. at 1592 (holding statute prohibiting visual depictions of animal cruelty unconstitutionally restrictive of protected speech).

216. See Benkler, Wealth of Networks, supra note 121, at 213–15 (arguing internetworked world provides "significant improvements" over mass media by drastically reducing entry costs of becoming a publisher and allowing anyone with internet access to comment on matters of public concern); see also Lawrence Lessig, The Future of Ideas 14 (2001) ("The right to criticize a government official is a resource that is not, and should not be, controlled . . . . No modern phenomenon better demonstrates the importance of free resources to innovation and creativity than the Internet."). But see Bollinger, supra note 106 (arguing democratic value of press as challenger of authority dependent on power of press as institution).

democratic discourse.[217] But the Court's reluctance to broadly define and grant special privileges to "the press," combined with a failure to explicitly relieve ordinary citizens from liability for third-party illegality, has distanced independent commentators from the holdings of cases like *Bartnicki* and *New York Times Co. v. Sullivan*.[218] The threat of criminal liability for federal identity fraud therefore hangs particularly heavy over independent commentators, chilling public discourse and potentially infringing on constitutionally protected speech.

3. Beyond Barrett Brown: The Sony Pictures and Celebrity-Photo Hacks. — Two recent incidents serve to highlight challenges posed by massive dumps of confidential information and the potential for enforcement against individuals responsible for disseminating those documents: the 2014 celebrity-photo hack and the 2014 Sony Pictures Entertainment (SPE) hack. Though these cases deal with different victims, motives, and information, each resulted in the unauthorized disclosure and dissemination of massive amounts of confidential information.

The 2014 celebrity-photograph hack has been called the largest online disclosure of celebrities' personal information in history and was widely discussed as an egregious violation of privacy.[219] On August 30, 2014, an anonymous hacker posted nude photographs of several major celebrities on the website 4chan.[220] Links to the images and the images themselves were subsequently distributed on social media and reported by major news outlets,[221] raising the strong implication that stolen images or hyperlinks to those images were either viewed by or disseminated by both bloggers and institutional journalists.[222] Though celebrities have

---

217. See, e.g., Benkler, Free Irresponsible Press, supra note 107, at 362–63 (arguing suppression of independent online media outlets "would severely undermine the quality of our public discourse").

218. 376 U.S. 254, 270, 279–80 (1964) (holding public official unable to recover for defamation unless publication was done with "'actual malice'" and commenting "debate on public issues should be uninhibited, robust, and wide-open").

219. Alex Hern & Dominic Rushe, Google Threatened with $100M Lawsuit over Nude Celebrity Photos, Guardian (Oct. 2, 2014, 8:21 AM), http://www.theguardian.com/technology/2014/oct/02/google-lawsuit-nude-celebrity-photos (on file with the *Columbia Law Review*) (describing event as "largest celebrity hacking scandal in history").

220. See Press Release, Apple, Apple Media Advisory: Update to Celebrity Photo Investigation (Sept. 2, 2014), http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html (on file with the *Columbia Law Review*) (discussing preliminary findings in Apple's investigation of celebrity-photo hack); see also Mike Isaac, Nude Photos of Jennifer Lawrence Are Latest Front in Online Privacy Debate, N.Y. Times (Sept. 2, 2014), http://www.nytimes.com/2014/09/03/technology/trove-of-nude-photos-sparks-debate-over-online-behavior.html (on file with the *Columbia Law Review*) (discussing origin of photo hack).

221. See Isaac, supra note 220 (discussing celebrity-photo hack and media response).

222. Some news outlets even chose to directly hyperlink to the stolen images in their reports. See, e.g., Dayna Evans, J-Law, Kate Upton Nudes Leak: Web Explodes over Hacked Celeb Pics, Gawker (Aug. 31, 2014, 6:30 PM), http://gawker.com/internet-explodes-over-j-

threatened ISPs with legal action based on the DMCA,[223] copyright claims based on the DMCA would likely be ineffective against news outlets and individuals. Victims must therefore find another means of civil or criminal redress against those disseminating the photographs; given at least some statements regarding intent to "prosecute,"[224] the federal identity-fraud statutes may provide the only mechanism to impose criminal liability.[225]

The SPE hack in November 2014 also resulted in a massive disclosure of confidential information obtained by a group of hackers, but it involved the dissemination of a greater variety of information.[226] The hackers stole and released thousands of social security numbers, credit card numbers, and passports—documents that undoubtedly fall within the definitions of §§ 1028 and 1028A—but many media reports focused on information obtained from SPE emails.[227] Due to widespread coverage of information contained in the confidential dump, SPE retained noted litigator David Boies and demanded media outlets delete any "stolen information" reported on.[228] This incident and related litigation threats should therefore clearly illustrate the danger of the government's argument in *United States v. Brown*: If hyperlinking to the massive dump of confidential documents from SPE constitutes identity fraud, even if the hyperlinks are shared only internally among the news team at the

---

laws-alleged-hacked-nudes-1629093854 (on file with the *Columbia Law Review*) (providing hyperlink to stolen photos on 4chan).

223. See, e.g., Hern & Rushe, supra note 219 (discussing DMCA lawsuit against Google).

224. See, e.g., Paul Farrell, Nude Photos of Jennifer Lawrence and Others Posted Online by Alleged Hacker, Guardian (Aug. 31, 2014, 11:33 PM), http://www.theguardian.com/world/2014/sep/01/nude-photos-of-jennifer-lawrence-and-others-posted-online-by-alleged-hacker (on file with the *Columbia Law Review*) (quoting Lawrence's publicist as stating "authorities have been contacted and will prosecute anyone who posts the stolen photos").

225. See supra Part II.A–B (discussing federal identity-fraud statutes and hacktivism).

226. See Press Release, Identity Finder, Identity Finder Research Uncovers Depth of Sony Breach (Dec. 5, 2014), http://www.identityfinder.com/us/Press/20141204210449 (on file with the *Columbia Law Review*) (detailing personal information released in SPE hack); Letter from Sony Pictures Entm't to Emps. of Sony Pictures Entm't (Dec. 8, 2014), available at http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf (on file with the *Columbia Law Review*) (informing SPE employees of extent of data breach).

227. See, e.g., Cecilia Kang, Craig Timberg & Ellen Nakashima, Sony's Hacked E-mails Expose Spats, Director Calling Angelina Jolie a 'Brat,' Wash. Post (Dec. 11, 2014), http://www.washingtonpost.com/business/economy/sonys-hacked-e-mails-expose-spats-director-calling-angelina-jolie-a-brat/2014/12/10/a799e8a0-809c-11e4-8882-03cf08410beb_story.html (on file with the *Columbia Law Review*) (discussing media coverage of Hollywood feuds revealed by SPE hack).

228. See, e.g., Michael Cieply & Brooks Barnes, Sony Pictures Demands that News Agencies Delete 'Stolen' Data, N.Y. Times (Dec. 14, 2014), http://www.nytimes.com/2014/12/15/business/sony-pictures-demands-that-news-organizations-delete-stolen-data.html (on file with the *Columbia Law Review*) (acknowledging receipt of letter from Boies on behalf of SPE requesting deletion of all data obtained from SPE hack).

New York Times or *Washington Post*, dozens of journalists and bloggers will be exposed to serious criminal liability under federal law.

III. RECONCILING IDENTITY-FRAUD PROSECUTION WITH THE FIRST AMENDMENT

As discussed throughout Part II, there are several ways to frame First Amendment challenges in the context of identity fraud. One approach is to view the sharing of confidential documents through the lens of the intellectual property cases discussed in Part II.B.2.[229] This approach requires determining whether sharing specific information constitutes "traffic[king]" in the actual "means of identification"[230] or "authentication features"[231] and, if so, whether prosecution constitutes an unconstitutional restriction on protected speech.[232] Prohibitions on sharing confidential personal information may also be troubling where such information was unlawfully obtained by a third party but subsequently accessed or shared as a matter of public concern by another.[233] Finally, on a more theoretical level, sharing information via hyperlink may be viewed as a uniquely expressive mode of communication warranting special protection akin to that afforded print publication in *New York Times v. Sullivan*.[234]

Regardless of how these statutory issues are framed, unconstitutional restrictions on protected speech may be avoided in several ways. Part III.A argues the First Amendment doctrines of overbreadth and vagueness may warrant invalidation of §§ 1028 and 1028A, though overbreadth is generally seen as "strong medicine" and rarely invoked. Part III.B argues the most effective way to avoid First Amendment challenges to §§ 1028 and 1028A is narrowly redefining the terms of § 1028(d) and heightening the mens rea requirement for provisions vulnerable to abuse. Part III.C then concludes by arguing First Amendment challenges to the federal identity-fraud regime should be reviewed using strict scrutiny when prohibitions on hyperlinking occur.

---

229. See supra Part II.B.2 (discussing hyperlinking and various forms of providing access in copyright, anticircumvention, and trademark infringement contexts).

230. 18 U.S.C. § 1028A (2012) (prohibiting trafficking in "means of identification").

231. Id. § 1028 (prohibiting trafficking in "authentication features").

232. See supra notes 154–176 (discussing hyperlinking in context of copyright infringement, trademark infringement, and anticircumvention under DMCA). The intellectual property cases generally provide substantial protection for hyperlinking to infringing content unless the hyperlink is provided for the sole purpose of infringement. Id.

233. See Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) (holding third-party individual's illegal conduct in obtaining information does not defeat First Amendment right to publish information of public concern by individual who played no role in illegality); see also supra notes 196–211 and accompanying text (discussing *Bartnicki, Ostergren,* and *Daily Mail* principle in greater depth).

234. See supra note 162 and accompanying text (discussing briefly Dalal's proposed framework for addressing hyperlinks within First Amendment).

A. *Vagueness and Overbreadth*

As discussed in Part I.B, the statutory definitions of "means of identification"[235] and "authentication features"[236] are extraordinarily broad—practically *any* name, string of numbers, or feature of an identification document may be regulated.[237] First Amendment challenges to §§ 1028 and 1028A may therefore rely on the breadth of these terms in arguing laws are overbroad[238] and unconstitutionally vague.[239] The "overbreadth" and "void-for-vagueness" doctrines are closely related and rooted in the average citizen's ability to recognize the precise conduct prohibited by criminal statutes.[240]

The fundamental premise of overbreadth doctrine is that narrowly defined statutory terms are required to avoid sweeping restrictions on protected speech.[241] Overbroad restrictions chill otherwise protected speech by individuals attempting to avoid liability.[242] Many of Barrett Brown's supporters focused on variations of this argument, claiming aggressive prosecution will result in a chilling effect on journalists and ordinary citizens.[243] There is some merit to this argument, as

---

235. 18 U.S.C. § 1028(d)(1) (defining "authentication feature" as "any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature").

236. Id. § 1028(d)(7) (defining "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual").

237. See supra notes 47–58 and accompanying text (discussing statutory definitions of "means of identification" and "authentication features" and policy considerations behind breadth of definitions).

238. See Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 494 (1982) (observing courts must determine whether enactment restricts substantial area of constitutionally protected conduct).

239. See Kolender v. Lawson, 461 U.S. 352, 357 (1983) ("[T]he void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement."); *Hoffman Estates*, 455 U.S. at 494–95 (holding "void-for-vagueness" doctrine generally requires determination statute is unconstitutionally vague in all applications).

240. See Stuart Buck & Mark L. Rienzi, Federal Courts, Overbreadth, and Vagueness: Guiding Principles for Constitutional Challenges to Uninterpreted State Statutes, 2002 Utah L. Rev. 381, 385, 388 (observing "void-for-vagueness" doctrine rooted in need for clear criminal statutes and "overbreadth" doctrine rooted in need to avoid prohibiting or chilling constitutionally protected conduct).

241. See *Hoffman Estates*, 455 U.S. at 494–95 (observing interaction between vagueness and overbreadth in chilling protected speech).

242. See Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973) (discussing chilling effects of enforcing unconstitutionally broad prohibition on speech); see also Gooding v. Wilson, 405 U.S. 518, 521 (1972) (observing overbreadth may deter law-abiding citizens from exercising right to engage in protected speech due to fear of criminal prosecution).

243. See, e.g., Kevin M. Gallagher, Why Barrett Brown's Trial Matters, Huffington Post: The Blog (Dec. 17, 2013, 5:26 PM), http://www.huffingtonpost.com/kevin-m-gallagher/why-barrett-brown-matters_b_4447315.html (on file with the *Columbia Law Review*) (last

demonstrated by the government's recent assertion that even email addresses may constitute "means of identification" giving rise to prosecution when misused.[244] But since invocation of the overbreadth doctrine is generally viewed as "strong medicine," it is unclear whether potential restrictions on protected speech outweigh the inconvenience and disruption of facially invalidating a criminal statute.[245] For such an argument to be seriously considered, those subject to prosecution must demonstrate unconstitutional restrictions on individuals with more straightforward cases. While Brown's case may not lend itself to reevaluating decades of statutory interpretation, indictment of an individual for genuinely journalistic activity might.[246]

The closely related "void for vagueness" doctrine requires that criminal statutes be defined with sufficient clarity to inform ordinary citizens of the conduct prohibited.[247] When coupled with the broad definitions of § 1028(d),[248] a plausible argument exists that the statute fails to inform ordinary citizens of precisely what conduct is prohibited, thereby encouraging arbitrary enforcement and necessitating facial invalidation.[249] Indeed, concerns regarding the breadth and vagueness of the

---

updated Feb. 16, 2014, 5:59 AM) (arguing Brown's detention has already had chilling effects on journalism).

244. See Brief for Appellee at 65–66, United States v. Auernheimer, 748 F.3d 525 (3d Cir. Sept. 20, 2013) (No. 13-1816) (arguing email addresses may constitute "means of identification" in certain circumstances).

245. See Virginia v. Hicks, 539 U.S. 113, 119–20 (2003) (holding likelihood of unconstitutional application must be "substantial" to outweigh legitimate social costs of preventing constitutional application); City Council v. Taxpayers for Vincent, 466 U.S. 789, 800–01 (1984) (holding a finding of substantial overbreadth based on "realistic danger" statute will compromise protected First Amendment rights of parties not appearing before court); *Broadrick*, 413 U.S. at 613 (recognizing concept of unconstitutionally overbroad application and asserting doctrine is "strong medicine" to be used sparingly).

246. For example, cybersecurity bloggers may engage in similar conduct as Barrett Brown, though their journalistic credentials are stronger. See, e.g., Karen Weise, The Cybersecurity Blogger Hackers Love to Hate, Bloomberg Bus. (Jan. 16, 2014), http://www.businessweek.com/articles/2014-01-16/brian-krebs-the-cybersecurity-blogger-hackers-love-to-hate (on file with the *Columbia Law Review*) (discussing cybersecurity blogger Brian Krebs and infiltration of criminal groups for newsworthy stories).

247. See United States v. Williams, 553 U.S. 285, 306 (2008) (holding criminal statute unconstitutionally vague where incriminating factual circumstances unclear); Kolender v. Lawson, 461 U.S. 352, 357 (1983) (holding penal statutes must be defined with "sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement").

248. 18 U.S.C. § 1028(d)(1) (2012) (providing broad definition of "authentication feature"); id. § 1028(d)(7) (providing broad definition of "means of identification"); see also supra note 16 and accompanying text (providing definitions and discussing sheer coverage of statutory terms).

249. See Houston v. Hill, 482 U.S. 451, 465–67 (1987) (observing vague laws allowing for arbitrary enforcement do not provide "breathing space" required by First Amendment). While an alternative to facial invalidation may be to sever unconstitutionally overbroad and vague provisions of §§ 1028 and 1028A, it is unclear whether severance is available in the First Amendment context. See United States v. Salerno, 481 U.S. 739, 745

federal identity-fraud statutes have been raised since the original enactment of § 1028 in 1982.[250] While §§ 1028 and 1028A may be justifiably invoked where an individual transfers a hyperlink to documents containing credit card numbers, the statutory language appears to prohibit transfer of many other types of information as well—including email addresses, online usernames, or any unique numeric identifier.[251]

B. *Amending the Statutory Framework*

Identity fraud has evolved alongside technologies facilitating it, necessitating statutory amendments at watershed moments such as the dawn of the Internet.[252] Recent developments like social media and hacktivism may represent yet another watershed moment requiring congressional intervention.[253] As discussed in Part I.C of this Note, hacktivism and the increased availability of information have altered the flow of information online and resulted in complex interactions between different actors—sometimes exposing relatively passive participants to the same liability as malicious hackers.[254] Two potential amendments to §§ 1028 and 1028A may reduce this potential for abuse and prevent unconstitutional restrictions on protected speech: narrower definitions in § 1028(d) and a heightened intent requirement for certain provisions of § 1028(a).

As discussed in Part III.A, the most pressing concern with the federal identity-fraud regime is the sheer breadth of its statutory definitions.[255]

(1987) (carving out exception for facial invalidation in First Amendment contexts); see also Note, Overbreadth and Listeners' Rights, 123 Harv. L. Rev. 1749, 1761–62 (2010) (arguing overbreadth challenge in First Amendment context requires facial invalidation, and highlighting failure to resolve issue in existing literature).

250. See H.R. Rep. No. 97–802, at 19–20 (1982) (discussing additional views and reservations of Rep. Robert W. Kastenmeier related to breadth of statutory language and federalism concerns).

251. See supra note 17 and accompanying text (arguing email addresses and other identifying information constitute prohibited "means of identification").

252. Legal scholars have recognized the need for laws to adapt to technology and society since the early days of the Internet. See, e.g., Arthur R. Miller, Bruce Bromley Professor of Law, Harvard Law School, The Emerging Law of the Internet, Remarks at the University of Georgia School of Law (Nov. 14, 2002), *in* 38 Ga. L. Rev. 991, 992 (2004) (explaining law is "not a stranger to technology" or dealing with "social phenomenon" like Internet). As an area of law now inextricably associated with the Internet, identity crimes are no exception. See supra Part I.B (discussing evolution of identity fraud as federal crime and various amendments to statutory scheme in response to changes in technology and sociopolitical environment).

253. See, e.g., Andrea M. Matwyshyn, Hacking Speech: Informational Speech and the First Amendment, 107 Nw. U. L. Rev. 795, 813–28 (2013) (discussing First Amendment implications of hacking and security vulnerability revelations).

254. See supra notes 63–77 and accompanying text (discussing complex interactions between hackers, hacktivists, passive participants, and nonmalicious observers).

255. See supra Part III.A (discussing broad definitions of "means of identification" and "authentication features" in 18 U.S.C. § 1028(d) (2012)).

Amending § 1028(d) by narrowing these definitions would make prosecution for sharing documents such as customer lists and email addresses less likely, alleviating some concerns regarding restrictions on newsgathering as well.[256] An alternative approach to overbroad statutory definitions may come in the form of a federal media shield law, such as the one debated by Congress at the time this Note was drafted.[257] Incorporating a safe harbor provision for individuals whose newsgathering activities incidentally violate federal identity-fraud statutes may protect institutional journalists while avoiding harmful restraints on law enforcement. As a counterpoint, such a broad exception for "newsgathering activities" would raise similar concerns as the overbroad terms of §§ 1028 and 1028A.[258] Regardless, federal shield law proposals have explicitly left entities like WikiLeaks and noninstitutional commentators unprotected.[259]

Requiring intent under certain provisions of §§ 1028(a) and 1028A may help avoid arbitrary enforcement and conviction.[260] Section 1028(a)(2), for example, prohibits "knowingly transfer[ring] an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority."[261] Heightening the mens rea standard in this section by requiring *intent* that information be *used* for malicious purposes may refocus identity-fraud prosecutions on the law's original targets: identity thieves and individuals trafficking in identity features for entirely fraudulent or malicious purposes.[262] Requiring intent would raise

256. For example, if the definition of "means of identification" in § 1028(d)(7) included only enumerated examples instead of "any name or number," the statute would be applied in fewer circumstances that implicate protected speech.

257. Free Flow of Information Act of 2013, S. 987, 113th Cong. § 2 (2013) (as reported by S. Comm. on the Judiciary, May 16, 2013) (providing conditions for "disclosure of information by certain persons connected with the news media").

258. See supra Part III.A (discussing overbreadth and vagueness challenges to §§ 1028 and 1028A).

259. See supra note 103 and accompanying text (discussing proposed federal shield law, including narrow definition of protected entities that excludes organizations like WikiLeaks and nontraditional journalists). But despite the Free Flow of Information Act's narrow definition of "covered journalist," it also provides for judicial discretion to protect individuals who are not explicitly covered when such protection is "in the interest of justice and necessary to protect lawful and legitimate news-gathering activities under the specific circumstances of the case." S. 987 § 11(1)(B).

260. Strong arguments exist, however, that the "beyond a reasonable doubt" standard applied in criminal proceedings already serves this function. See In re Winship, 397 U.S. 358, 364 (1970) ("[W]e explicitly hold that the Due Process Clause protects the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged.").

261. 18 U.S.C. § 1028(a)(2).

262. H.R. Rep. No. 97-975, at 3 (1982) (discussing urgent need to prevent production and use of fraudulent identification due to use in "drug smuggling, illegal immigration, flight from justice, [and] fraud against business and the government").

several subsidiary questions, not least of all being "intent to do *what*?" The difficulty here is drafting a provision encompassing malicious use of identity information while avoiding the catch-all phrases that result in further overbreadth and vagueness.[263] These difficult questions also support arguments that an intent requirement enables malicious identity thieves to avoid prosecution and is therefore undesirable.[264]

C. *Strict Scrutiny for Hyperlinking Restrictions*

Though not necessarily an independent solution,[265] Dalal's framework for analyzing hyperlinks within the First Amendment context provides an interesting lens through which courts may analyze prosecution for identity fraud connected to sharing a hyperlink.[266] As briefly mentioned in Part II.B.2, Dalal argues that the standard of "actual malice" adopted in *New York Times Co. v. Sullivan*[267] should be extended to the hyperlinking context.[268] According to Dalal, the Internet has evolved in such a way that it now serves the same democracy-protecting function print media served at the time *Sullivan* was decided.[269] Therefore, regulation of hyperlinking as a vital communicative component of the Internet should be subject to strict scrutiny review.[270]

Strict scrutiny would require statutory prohibitions on hyperlinking to be "narrowly tailored to further compelling governmental inter-

---

263. For further reading on the challenges of drafting computer-specific criminal statutes, see generally Joseph M. Olivenbaum, <Ctrl><Alt><Delete>: Rethinking Federal Computer Crime Legislation, 27 Seton Hall L. Rev. 574, 590–91 (1997) (arguing focus on technology instead of harm results in overbreadth and imprecision).

264. See supra notes 47–58 and accompanying text (discussing congressional response to growing threat of identity theft with broad statutory prohibitions).

265. Application of strict scrutiny review would likely force adoption of statutory amendments to fulfill narrow tailoring requirements. See infra notes 271–277 and accompanying text (explaining strict scrutiny's requirement that laws be narrowly tailored to compelling government interest).

266. See Dalal, supra note 145, at 1075 (discussing First Amendment implications of hyperlinking and proposing strict scrutiny review of hyperlinking prohibitions).

267. 376 U.S. 254, 279–80 (1964) (holding public official unable to recover for defamation unless publication was done with actual malice); see also Hustler Magazine v. Falwell, 485 U.S. 46, 56–57 (1988) (extending *Sullivan* standard to intentional infliction of emotional distress on public figures).

268. See Dalal, supra note 145, at 1068–69 (arguing for standard similar to *Sullivan* for hyperlinking).

269. *Sullivan* is often characterized as a seminal "freedom of the press" case, though it is unclear whether this is an accurate characterization. See *Sullivan*, 376 U.S. at 282 (holding First Amendment protections regarding publication extended to "citizen-critic[s] of government" as well as institutional journalists).

270. Although defamation and intentional infliction of emotional distress are not necessarily analogous to identity fraud, Dalal—and, indeed, the Court in *Sullivan* and subsequent related opinions—focuses on the need to protect fundamental First Amendment rights as the purpose of the "actual malice" standard. See Dalal, supra note 145, at 1068–69 (discussing need to protect fundamental First Amendment rights).

ests."[271] The governmental interest behind identity-fraud statutes is undoubtedly compelling.[272] Narrowly tailoring statutes to further this interest, however, poses more difficult questions beyond the scope of this Note.[273] More interesting than the outcome in any particular factual scenario,[274] application of strict scrutiny to hyperlinking as a communicative medium addresses the core First Amendment concerns stemming from prosecution for hyperlinking to confidential information. While identity-fraud statutes serve compelling governmental interests, criminal prohibitions on hyperlinking that are *not* narrowly tailored to that interest threaten to restrict a communicative medium with unique democratizing and information-sharing value.[275]

Courts often respond to rapid technological change by trying to fit "old crimes into new bottles."[276] This understandable and cautious approach towards technology and law, however, seems to justify heightened review of matters fundamentally important to digital communication.[277] Where outdated criminal statutes are applied to new technologies and social trends, strict scrutiny protects First Amendment rights until legal implications are clearly understood. Applying this general principle to identity fraud, strict scrutiny review protects ordinary citizens and the right to access or share publicly available information, while allowing Congress to narrowly tailor provisions addressing malicious identity fraud.

---

271. Grutter v. Bollinger, 539 U.S. 306, 326 (2003) (applying strict scrutiny to racial classifications).

272. See Part I.B (discussing policy underpinnings of federal identity-fraud regime).

273. See supra notes 165–173 and accompanying text (discussing *Corley* court's unwillingness to address standard of review for First Amendment challenges to hyperlinking); see also Universal City Studios, Inc. v. Corley, 273 F.3d 429, 457 (2d Cir. 2001) (refusing to adopt strict scrutiny or trial court's test but holding "linking" prohibition sufficiently narrow to survive First Amendment challenge).

274. Indeed, some might argue very limited factual circumstances in the criminal context warrant strict scrutiny review of hyperlinking restrictions. Dalal explicitly discounts cases where hyperlinking *intentionally* facilitates illegal behavior. Dalal, supra note 145, at 1069 ("Extending such a constitutional privilege does not mean allowing linking when it clearly intends to facilitate illegal behavior.").

275. Unlike restrictions on blogs, wikis, or other web content, restrictions on hyperlinks undermine the core infrastructure and communicative value of the Internet. See Benkler, Wealth of Networks, supra note 121, at 218 (describing hyperlinking as "core characteristic of communication" on Internet); Porismita Borah, The Hyperlinked World, 19 J. Computer Mediated Comm. 576, 579 (2014) (highlighting unique importance of hyperlinks to newsgathering, source credibility, and information retrieval on Internet).

276. Michael Edmund O'Neill, Old Crimes in New Bottles: Sanctioning Cybercrime, 9 Geo. Mason L. Rev. 237, 239 (2000) (arguing cybercrimes may be dealt with by laws applicable to physical world).

277. See Benkler, Wealth of Networks, supra note 121, at 9 (arguing networked society greatly enhances individual autonomy); Dalal, supra note 145, at 1069 (arguing hyperlinking and Internet provide "important medium of communication that uniquely supports our free speech values").

CONCLUSION

Identity fraud is facilitated by rapid growth in technology and social trends, thereby necessitating periodic statutory revisions. Increased data mobility and the challenges of widespread hacktivism have resulted in significant new barriers to identity-fraud prosecution under the current framework. In addressing cases with potential implications for First Amendment rights, however, courts must carefully balance the need for aggressive prosecution of identity theft with the accompanying chilling effects on democratic discourse. The Internet now serves a uniquely valuable role in ensuring the free flow of information of public concern; without either judicial constraints on identity-fraud prosecution or statutory revisions to its outdated legal framework, arbitrary prosecution will remain a threat to independent commentators and ordinary citizens seeking to contribute to public discourse.