Northwestern Journal of Technology and Intellectual Property

Volume 13 | Issue 2 Article 1

2015

A Target to the Heart of the First Amendment: Government Endorsement of Responsible Disclosure as Unconstitutional

Kristin M. Bergman
Reporters Committee for Freedom of the Press

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

A Target to the Heart of the First Amendment: Government Endorsement of Responsible Disclosure as Unconstitutional

Kristin M. Bergman

May 2015 VOL. 13, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 13, Number 2 (May 2015)

A Target to the Heart of the First Amendment: Government Endorsement of Responsible Disclosure as Unconstitutional

By Kristin M. Bergman*

Brian Krebs, a former reporter for the Washington Post who is now known for his blog Krebs on Security, remained relatively unknown for most of his career. But in December 2013, Mr. Krebs found that hackers had exploited a data vulnerability in Target's electronic-payment system, compromising millions of credit-card numbers that had been used to purchase goods from the second-largest discount retailer in the United States. In the following months, an investigation revealed that the breach affected nearly half of the 110-million credit cards recently used at Target, resulting in one of the largest known digital credit-card heists in history.

Even before Target's data breach personally affected millions of consumers, concern over the security of personal data was endemic. A survey conducted in March 2013 revealed that 82.1% of Americans were at least somewhat worried about a data breach involving banks, government entities, or other organizations, and roughly the same percentage were concerned about identity theft and credit-card fraud. With over 78-million data records containing personal information exposed to breaches in the first ten months of 2014 alone, it is unsurprising that a separate survey found that 77% of consumers agreed that expeditious notification of vulnerabilities involving stolen or lost data was important. Coupled with the potential widespread harm caused by data breaches, discrepancies in data-holders' approaches to security vulnerabilities have prompted a call for a national response.

Generally, two approaches exist for confronting data security issues: full disclosure and responsible disclosure. Proponents of the former argue that stifling communication about data breaches or vulnerabilities, no matter the source, is detrimental, conflicting with both public sentiment and constitutional rights. On the other end of the spectrum, supporters of a responsible disclosure policy suggest that allowing companies to rectify data security issues before public dissemination provides a better solution. In effect, responsible disclosure requires those who discover a data vulnerability to not only notify the affected organization, but also keep knowledge of the data security weakness confidential, regardless of its potential impact on consumers.

---

* Post-Graduate Legal Fellow, Reporters Committee for Freedom of the Press. J.D., William & Mary School of Law, 2014; B.A., Brown University, 2011. I would first like to extend my thanks to Andy Sellars and Jeff Hermes for introducing me to this issue at the (now former) Digital Media Law Project, and for fostering and supporting my interest in media law. Many thanks also to Rebecca Green for her valuable insight, encouragement, and enthusiasm throughout the writing process, and to the staff of the *Northwestern Journal of Technology & Intellectual Property*.

Although the predominant industry approach, this Article argues that the responsible disclosure approach should not be legislatively or judicially adopted. Not only does a responsible disclosure policy violate the First Amendment as a prior restraint, but it also constitutes poor public policy, ultimately causing a chilling effect that would reduce business accountability. In an effort to avoid both limiting the development of enhanced data security safeguards and restricting the public's ability to engage in self-help, Congress and the judiciary should allow basic market forces to pave the way for innovation in this continually evolving field.

TABLE OF CONTENTS

I. INTRODUCTION

¶1 Brian Krebs, a former reporter for the *Washington Post* now known for his blog *Krebs on Security*,[1] remained relatively unknown for most of his career. But in December 2013, Mr. Krebs decided to do something that would affect millions of global consumers.[2] Mr. Krebs received information from two confidential sources in the banking industry noting a major increase in fraudulent credit-card purchases.[3] Investigating this spike in credit-card fraud, Mr. Krebs turned to underground online

[1] KREBS ON SECURITY, http://krebsonsecurity.com/ (last visited Mar. 21, 2014).
[2] *See* Nicole Perlroth, *Reporting from the Web's Underbelly*, N.Y. TIMES (Feb. 16, 2014), http://www.nytimes.com/2014/02/17/technology/reporting-from-the-webs-underbelly.html?hpw&rref=business&_r=0.
[3] *See id*.

forums, where he discovered a data security breach of unparalleled magnitude. With the help of his sources, Mr. Krebs found that hackers had exploited a data vulnerability in Target's electronic-payment system, compromising millions of credit-card numbers that had been used to purchase goods from the second-largest discount retailer in the United States. He ultimately concluded that "the breach extend[ed] to nearly all Target locations nationwide, and involve[d] the theft of data stored on the magnetic stripe of cards used at the stores," affecting millions of cardholders.[4]

¶2 Mr. Krebs first notified Target of the breach on December 18, 2013. But after "multiple requests for comment,"[5] Target refused to address his inquiries. Recognizing the importance of informing the public of this far-reaching security breach, Mr. Krebs decided to post information about the data breach on his blog.[6] The following morning Target announced the breach, confirming the "unauthorized access to Target payment card data."[7] In the following months, the investigation revealed that the breach affected nearly half of the 110-million credit cards recently used at Target, resulting in one of the largest known digital credit-card heists in history.[8] Reflecting on Mr. Krebs' role, Barmak Meftah, CEO of threat-detection service Alien Vault, stated,

> [Mr. Krebs is] doing the security industry an enormous favor by disseminating real-time threat information. . . . We are only as strong as our information. Unless we are very specific and effective about exchanging threat data when one of us gets breached, we will always be a step behind the attackers.[9]

Fortunately, Target was relatively quick to respond after notification of the breach, even if the discovery and initial public disclosure came from an individual outside the company. But this expeditious response is not the norm. For instance, in 2010, security researchers notified Skype—now, a division of Microsoft—of a data vulnerability that allowed users to be tracked through their IP addresses.[10] Despite notification of this data security weakness, Skype refused to address the issue for nearly a year, prompting the researchers to publish their findings, which in turn alerted the public of this vulnerability for the first time.[11]

---

[4] Brian Krebs, *Sources: Target Investigating Data Breach*, KREBS ON SECURITY (Dec. 18, 2013, 2:33 PM), http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.

[5] *See id*.

[6] *Id*.

[7] *A Message from CEO Gregg Steinhafel About Target's Payment Card Issues*, TARGET (Dec. 19, 2013), https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca.

[8] Hadley Malcolm, *Target Breach Helps Usher in New World of Data Security*, USA TODAY (Feb. 24, 2014, 5:22 PM), http://www.usatoday.com/story/money/business/2014/02/22/retail-hacks-security-standards/5257919/; *see also* Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY (May 6, 2014, 12:24 AM), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/ (reporting that seventy-million consumer records were stolen).

[9] Perlroth, *supra* note 2.

[10] *See* Joel Schectman, *Skype Knew of Security Flaw Since November 2010, Researchers Say*, WALL ST. J. (May 1, 2012, 8:06 PM), http://blogs.wsj.com/cio/2012/05/01/skype-knew-of-security-flaw-since-november-2010-researchers-say/.

[11] *See id*.

¶3 Over the past decade, data security issues have increasingly roused public concern. In the past two years alone, roughly half of all consumers have been notified of security breaches involving the loss of personal information.[12] Coupled with the potential widespread harm caused by data breaches, discrepancies in data-holders' approaches to security vulnerabilities have prompted a call for a national response. In the U.S. Senate Judiciary Committee's hearing on *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*,[13] Senator Mike Lee recognized, "I generally trust the market to create the right incentives for retailers to protect data of their customers. But consumers need notification of data breaches for that to work. . . . One possible legislative response is to codify a national standard for data security."[14] In light of this hearing and the Target data breach, former Attorney General Eric Holder urged Congress to enact cybersecurity legislation encouraging heightened data security, including a "strong national standard" with a company-notification requirement when data has been compromised.[15] Though Mr. Holder's recommendations focused on disclosure requirements for data-hosting companies, Congress could promulgate similar standards for those who discover weaknesses or breaches in data security, thus reinforcing the efficacy of any data security legislation.[16]

¶4 Generally, two approaches exist for confronting data security issues: full disclosure and responsible disclosure. Proponents of the former argue that stifling communication about data breaches or vulnerabilities, no matter the source, is detrimental, conflicting with both public sentiment and constitutional rights. They acknowledge but accept the

[12] EMC CORP., CONSUMER PERCEPTIONS ON SECURITY: DO THEY STILL CARE? (2014), *available at* http://www.emc.com/collateral/brochure/consumer-perceptions-on-security.pdf.

[13] Letter from Am. Bankers Ass'n et al. to Sen. Patrick Leahy, Chairman, Comm. on the Judiciary, and Sen. Charles Grassley, Comm. on the Judiciary (Feb. 3, 2014), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=138603a26950ad873303535a6300170f.

[14] *Summary: Target Testifies on Massive Data Breach*, WALL ST. J. (Feb. 4, 2014, 10:38 AM), http://blogs.wsj.com/corporate-intelligence/2014/02/04/live-target-testifies-on-massive-data-breach/.

[15] Schuyler Velasco, *Eric Holder Urges New Laws for Data Breaches After Target Attack*, CHRISTIAN SCI. MONITOR (Feb. 24, 2014), http://www.csmonitor.com/Business/2014/0224/Eric-Holder-urges-new-laws-for-data-breaches-after-Target-attack-video. Over the last decade, most states have passed notification laws requiring certain data-holders to inform consumers of security breaches in writing; however, these laws are traditionally limited in applicability to situations in which personally identifiable information was actually exposed. *See State Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated Aug. 20, 2012).

[16] Disclosure of data has been central in discussions of proposed cybersecurity bills. *See, e.g.,* Data Security Act of 2014, S. 1927, 113th Cong. (2014); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014); Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. (2013) (permitting delayed disclosure "to avoid interfering with a civil or criminal investigation or threatening national or homeland security"). However, no consensus has been found between parties to allow passage. *See* Alina Selyukh, *Will Congress Require Companies to Share Data on Cyber-Security Breaches?*, CHRISTIAN SCI. MONITOR (Apr. 30, 2014), http://www.csmonitor.com/USA/Latest-News-Wires/2014/0430/Will-Congress-require-companies-to-share-data-on-cyber-security-breaches. With President Obama's renewed emphasis on cybersecurity, perhaps a relevant law will finally be enacted in 2015. President Barack Obama, State of the Union Address (Jan. 20, 2015), *available at* http://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015 ("And tonight, I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information."); *see also Safeguarding American Consumers & Families*, WHITE HOUSE (Jan. 12, 2015), http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

risk of exploitation. On the other end of the spectrum, supporters of a responsible disclosure policy suggest that allowing companies to rectify data security issues before public dissemination provides a more effective solution. Responsible disclosure requires those who discover a data vulnerability to not only notify the affected organization, but also keep knowledge of the data security weakness confidential, regardless of its potential impact on consumers.

¶5 Although the predominant industry approach, this Article argues that the responsible disclosure approach should not be legislatively or judicially adopted.[17] Not only does a responsible disclosure policy violate the First Amendment as a prior restraint, but it also constitutes poor public policy, ultimately causing a chilling effect that would reduce business accountability. Further, while Target's remedial measures worked, it is easy to imagine what might have transpired if Mr. Krebs had not published his discovery after confirming Target's data breach. No record exists of how many consumers were able to take action in the hours following Mr. Krebs's revelation to prevent credit-card fraud, making it impossible to gauge how much damage would have occurred if Mr. Krebs had not forced Target's hand to disclose the breach. Worse yet, as the law currently stands, those who expose data vulnerability issues are often subject to both civil and criminal liability, such as under the Computer Fraud and Abuse Act.

¶6 In sum, it would be inappropriate for the government—whether by an act of Congress or a judicial order—to adopt a responsible disclosure policy, delaying or otherwise hindering the publication of news about data security vulnerabilities and breaches. Part II begins the analysis with additional background on disclosure policies and prior opportunities for government endorsement of a policy. Part III then applies the First Amendment's prior restraint doctrine to limitations on vulnerability speech. Part IV turns to editorial protections specific to the press, while Part V considers the policy arguments against adopting responsible disclosure. Part VI concludes with consideration of other relevant legal concerns, such as contract and agency law.

II. BACKGROUND

A. Vulnerability Disclosure Policies

¶7 For the past fifteen years, an avid policy debate has ruminated within the technology community over the best way to approach the discussion and publication of data security issues.[18] Many recognize the myriad advantages of publishing news about security weaknesses and breaches, including better data-holder accountability, increased knowledge among consumers, opportunity for peer review, faster resolution of data vulnerabilities, and the development of improved security measures.[19] On the other hand, a policy mandating confidentiality of data breaches has its benefits. For instance, immediate public disclosure interferes with a company's ability to resolve vulnerabilities

[17] *See* Scott Berinato, *Software Vulnerability Disclosure: The Chilling Effect*, CSO (Jan. 1, 2007, 7:00 AM), http://www.csoonline.com/article/2121727/application-security/software-vulnerability-disclosure--the-chilling-effect.html.

[18] *See Vulnerability Disclosure Publications and Discussion Tracking*, UNIV. OF OULU, https://www.ee.oulu.fi/research/ouspg/Disclosure_tracking (last visited Aug. 14, 2014) (tracking the debate between models of vulnerability disclosure from 1997 to present day).

[19] *See infra* Part V(A)–(B).

discreetly without causing reputational or financial harm. Further, public disclosure might encourage criminals to exploit newly exposed security vulnerabilities before the data-holder is able to create a patch. Bruce Schneier, a data security expert, summarizes this debate, asking:

> Is the benefit of publicizing an attack worth the increased threat of the enemy learning about it? Should we reduce the Window of Exposure by trying to limit knowledge of the vulnerability, or by publishing the vulnerability to force vendors to fix it as quickly as possible?[20]

¶8 Discussed previously, two disclosure policies have developed within this debate—full disclosure and responsible disclosure. Perhaps, however, it is best to understand these policies as ends of a spectrum rather than discrete alternatives. Full disclosure is the "practice of making the details of security vulnerabilities public."[21] In contrast, many refer to a delayed public-disclosure policy as "responsible disclosure" or "coordinated vulnerability disclosure."[22] Though company policies vary, most require the security researcher who discovers a vulnerability to notify the company of the vulnerability first, and then delay (or resist) public disclosure, giving the company an opportunity to remedy the problem before publication.[23]

¶9 Over the past few decades, disclosure policies have evolved alongside technology. Although nondisclosure was originally the norm, full disclosure gained prominence in the 1980s, remaining the dominant stance for over a decade.[24] As the twenty-first century progresses, however, more vendors and researchers are embracing the responsible disclosure movement.[25]

---

[20] Bruce Schneier, *Full Disclosure of Security Vulnerabilities a "Damned Good Idea*," CSO (Jan. 9, 2007), http://www.csoonline.com/article/216205/schneier-full-disclosure-of-security-vulnerabilities-a-damned-good-idea. Schneier describes the Window of Exposure to "explain the evolution of a security vulnerability over time" in terms of "a graph of danger versus time, [with] the Window of Exposure as the area under the graph." *Id*.

[21] *Id.*; *see also* Brian Deline, *Full Disclosure*, SANS INST. (Nov. 28, 2000), http://web.archive.org/web/20010210204159/http://www.sans.org/infosecFAQ/hackers/disclosure.html.

[22] *See, e.g., Coordinated Vulnerability Disclosure*, MICROSOFT SECURITY RESPONSE CTR., http://www.microsoft.com/security/msrc/report/disclosure.aspx (last visited Aug. 21, 2014); ORG. FOR INTERNET SAFETY, GUIDELINES FOR SECURITY VULNERABILITY REPORTING & RESPONSE 6 (2004), *available at* http://www.oisafety.org/reference/process.pdf.

[23] *See* Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 NW. U. L. REV. 795, 845 n.154 (2013); Bruce Schneier, *Crypto-Gram*, SCHNEIER ON SECURITY (Nov. 15, 2001), https://www.schneier.com/crypto-gram-0111.html#1. Microsoft and Scott Culp led the way in adopting such a delayed-publication policy. *Coordinated Vulnerability Disclosure*, *supra* note 22; ORG. FOR INTERNET SAFETY, *supra* note 22. More recently, Google adopted a policy to address security researchers' discoveries of new data vulnerabilities with a more aggressive timeline for companies to resolve the security vulnerability or notify their users. *See* Chris Evans & Drew Hintz, *Disclosure Timeline for Vulnerabilities Under Active Attack*, GOOGLE ONLINE SECURITY BLOG (May 29, 2013), http://googleonlinesecurity.blogspot.ro/2013/05/disclosure-timeline-for-vulnerabilities.html.

[24] Schneier, *supra* note 20.

[25] *See Q&A with Bruce Schneier*, BERKMAN CTR. (Nov. 25, 2013), *available at* http://cyber.law.harvard.edu/node/8665.

B. Disclosure and the Courts

¶10 Dr. Andrea M. Matwyshyn recently coined the term "vulnerability speech," or "informational speech that identifies a potentially critical flaw in a technological system or product but also indirectly potentially facilitates criminality."[26] Invoking this language, the debate over vulnerability disclosure policies should be understood as a debate over the proper scope of vulnerability speech and its potential regulation. Yet, despite the growing popularity and importance of this debate, few courts have had the opportunity to address the matter, and no court has issued a definitive answer.

1. MBTA v. Anderson

¶11 In 2008, three students at the Massachusetts Institute of Technology (MIT) discovered a vulnerability in the Massachusetts Bay Transportation Authority's (MBTA) transit-payment system.[27] In doing so, the students reverse engineered the magnetic stripe on passenger tickets to hack the MBTA-provided smartcard, allowing them to access vital, nonpublic information.[28] Planning to present at DEFCON, a conference for hackers,[29] the MIT students wished to expose the weaknesses in the MBTA's system by demonstrating the process they used and releasing the open-source tools they wrote while researching the MBTA system.[30]

¶12 Before the presentation, the MBTA filed suit in the U.S. District Court for the District of Massachusetts to enjoin the students from presenting at DEFCON or otherwise publically exposing the fare-payment system's vulnerability.[31] The MBTA's complaint

---

[26] Matwyshyn, *Hacking Speech*, *supra* note 23, at 798 (invoking and adopting Martin Redish's language of "informational speech"). Though a compelling issue, this Article will not address the role of code in vulnerability speech and the potential implications it may have on First Amendment protection and analysis.

[27] Kim Zetter, *DefCon: Boston Subway Officials Sue to Stop Talk on Fare Card Hacks—Update: Restraining Order Issued; Talk Cancelled*, WIRED (Aug. 08, 2008, 11:45 PM), http://www.wired.com/threatlevel/2008/08/injunction-requ/.

[28] *See id*.

[29] *Speakers for DEFCON16*, DEFCON, https://www.defcon.org/html/defcon-16/dc-16-speakers.html#Anderson (last visited Mar. 22, 2014). The students planned to present on "The Anatomy of a Subway Hack: Breaking Crypto RFIDs & Magstripes of Ticketing Systems." *See id*.

[30] *See id*. The MIT students explained:

> In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We survey "human factors" that lead to weaknesses in the system, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote in the process of researching these attacks. With live demos, we will demonstrate how we broke these systems.

Id.

[31] Complaint at 16, Mass. Bay Transp. Auth. v. Anderson, No. 08-CA-11364-GAO (D. Mass. 2008), 2008 WL 6954941, *available at* https://www.eff.org/node/55690. The Electronic Frontier Foundation, which represented the students, has all of the relevant court documents for this case available for viewing and download on its site. ELEC. FRONTIER FOUND., https://www.eff.org/cases/mbta-v-anderson (last visited

alleged a violation of the Computer Fraud and Abuse Act (CFAA), arguing that the students accessed the MBTA's systems without authorization and that disclosure before allowing the MBTA to resolve the vulnerability internally would cause irreparable harm to the city's transit system.[32] Though the students insisted they did not intend to reveal sufficient details for someone to attack the MBTA system,[33] the district court granted a ten-day temporary restraining order,[34] preventing the students from presenting at DEFCON.[35] The MBTA also filed a motion for a preliminary injunction—essentially to continue the temporary restraining order—but the court refused and vacated the restraining order.[36] In an oral decision, Judge O'Toole declined, as a matter of statutory construction, to extend CFAA liability to this vulnerability speech.[37] Unfortunately for the students, the decision came too late: the MBTA had effectively silenced them.

¶13 Although Judge O'Toole avoided addressing First Amendment concerns, he nevertheless detailed the various policy rationales inherent to the vulnerability disclosure debate. The judge recognized:

> [T]here's obviously interest in protecting the integrity of the fare system, in avoiding major loss to the MBTA. That's certainly legitimate harm to be concerned about. There's an interest and a potential harm to persons in the position of the defendants regarding their ability to engage in public discussions about these matters. And I make that point in the first instance without reference to the First Amendment, what it may or may not guarantee under these circumstances; that is, I think the harm exists as a practical matter without consideration of whether it's something that also implicates the person. In other words, I think this matter can be resolved without resort to constitutional principles at this stage.[38]

Though the court did not invoke the First Amendment, it ultimately protected the students' interests in vulnerability speech and the public's "right to know."[39]

Mar. 22, 2014).

[32] Complaint at 12, Mass. Bay Transp. Auth. v. Anderson, No. 08-CA-11364-GAO.

[33] Kim Zetter, *Federal Judge in DefCon Case Equates Speech with Hacking: Updated with Recording from Hearing*, WIRED (Aug. 10, 2008, 3:55 AM), http://www.wired.com/threatlevel/2008/08/eff-to-appeal-r/.

[34] Temporary Restraining Order at 2, Mass. Bay Transp. Auth. v. Anderson, No. 08-CA-11364-GAO ("That the MIT Undergrads are hereby enjoined and restrained, in accordance with Fed. R. Civ P. 65(b)(2), from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System.").

[35] Ironically, the MBTA's vulnerability report presented to obtain the temporary restraining order—and therefore made public when the order was granted—provided more information about the MBTA system's security susceptibilities than the MIT students' presentation would have disclosed. *See* Zetter, *supra* note 33.

[36] *See* Transcript of Aug. 19, 2008 Motion Hearing at 5, Mass. Bay Transp. Auth. v. Anderson, No. 08-CA-11364-GAO; *see also* Zetter, *supra* note 33.

[37] *See* Transcript of Aug. 19, 2008 Motion Hearing at 34, Mass. Bay Transp. Auth. v. Anderson, No. 08-CA-11364-GAO.

[38] *Id.* at 63.

[39] *See id*.; *see also* Thomas I. Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U. L. Q. 1 (1976) (describing the evolution of a right to know, or right to receive information, under the First Amendment).

¶14 Although a limited decision, the fact that Judge O'Toole recognized the value of vulnerability speech could deter courts from issuing similar injunctions in the future. Nevertheless, the district court's initial injunction demonstrates the possibility of a court deciding to adopt a delayed-disclosure approach without properly accounting for the far-reaching and unpredictable consequences of such a decision. Discussed next, a similar opportunity recently came before the Third Circuit Court of Appeals.

2. United States v. Auernheimer

¶15 Two years after the MBTA incident, Andrew Auernheimer and Daniel Spitler—both members of Goatse Security, a consulting firm of semiautonomous security researchers—revealed a data vulnerability in AT&T's computer system that exposed iPad owners' personal information just two months after the product was released. [40] They discovered that an HTTP request on AT&T's website could match the iPad owner's Integrated Circuit Card Identifier (ICC-ID)[41] with the iPad owner's email address.[42] After manually entering a few individual ICC-IDs, Auernheimer and Spitler wrote a script that systematically generated possible ICC-IDs, allowing them to harvest over 110,000 subscribers' email addresses.[43]

¶16 Immediately upon discovering the vulnerability, Auernheimer approached several major news outlets, including the *News Corporation*, the *San Francisco Chronicle*, the *Washington Post*, and *Thomson-Reuters*, before *Gawker* agreed to publish news of the vulnerability.[44] By the following day, however, AT&T had corrected the vulnerability, and the FBI had launched an investigation into the breach.[45] In response to criticism over the disclosure, Goatse Security released a statement:

> This disclosure needed to be made. iPad 3G users had the right to know that their email addresses were potentially public knowledge so they could take steps to mitigate the issue (like changing their email address). This was done in service of the American public. . . . All data was gathered from a public webserver with no password, accessible by anyone on the

[40] *See* Ryan Tate, *Apple's Worst Security Breach: 114,000 iPad Owners Exposed*, GAWKER (June 9, 2010, 4:50 PM), http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed. Andrew Auernheimer is also known as "Weev." *Id.*

[41] *See id.* Essentially, an ICC-ID is a device identification number stored on the SIM card to identify the unique account. This automatically integrates with the website's URL upon accessing the tablet.

[42] *See id*.

[43] *See id*.; Matt Buchanan, *The Little Feature That Led to AT&T's iPad Security Breach*, GIZMODO (June 9, 2010, 9:19 PM), http://gizmodo.com/5559686/the-little-feature-that-led-to-atts-ipad-security-breach.

[44] *See* Superseding Indictment at 12, United States v. Auernheimer, No. 11-CR-470 SDW (D.N.J. Aug. 16, 2012), 2012 WL 6676870; *see also* Tate, *supra* note 40. It is worth noting that in a later interview, Auernheimer mentioned that they only gave *Gawker* the data "because he agreed he would censor the ICC-IDs and the emails so they couldn't be used to compromise anything." Elinor Mills, *Hacker Defends Going Public with AT&T's iPad Data Breach (Q&A)*, CNET (June 10, 2010, 4:12 PM), http://www.cnet.com/news/hacker-defends-going-public-with-at-ts-ipad-data-breach-q-a/.

[45] *See* Tate, *supra* note 40.

> Internet. There was no breach, intrusion, or penetration, by any means of the word.[46]

¶17 Although Goatse Security asserted that its security researchers had acted in the public interest, AT&T and the FBI felt otherwise. In early 2011, an FBI investigation led to a criminal complaint filed against Spitler and Auernheimer, alleging they committed fraud and violated the CFAA.[47] Moreover, the misdemeanor CFAA charge was elevated to a felony because New Jersey state law considers accessing a computer without authorization and disclosing any data obtained from such unauthorized access a criminal offense.[48] While Spitler pled guilty, Auernheimer chose to fight the indictment, seeking absolution from accusations he felt were unjust.[49] Ultimately, a jury found Auernheimer guilty on all counts, resulting in a forty-one-month prison sentence and a fine of $73,167.[50] He appealed his case to the Third Circuit Court of Appeals,[51] wherein various parties chose to file amicus briefs concerning the potentially widespread consequences of the court's ruling.[52]

¶18 While the Third Circuit's decision eventually pivoted on procedural issues, the district court's ruling prompted various advocates of First Amendment protection to interject. For instance, many criticized the district court's rejection of Auernheimer's invocation of First Amendment protection: the court decided that the information conveyed, being both private and integral to the criminal conduct, was not protected by the First Amendment.[53] In an amicus brief, the Berkman Center's Digital Media Law Project (DMLP)[54] argued that elevating the CFAA count from a misdemeanor to a felony for disclosing true information of public concern required the court to satisfy First Amendment scrutiny.[55] Perhaps most important, the DMLP encouraged the appellate court to exercise restraint in endorsing a particular stance in the vulnerability disclosure debate:

> Preventing punishment in this case absent satisfaction of First Amendment scrutiny also ensures that the government does not have too great a hand in interfering with the ethics and norms of the data security community, who are currently engaged in a robust debate over when it is appropriate to tell a company first about bad data practices, and when it is better to inform the public directly . . . . Prosecutors and lawmakers should not use

---

[46] Ryan Tate, *FBI Investigating iPad Breach (Update)*, GAWKER (June 10, 2010, 7:15 PM), http://gawker.com/5560542/fbi-investigating-ipad-breach.

[47] *See* Complaint at 2, United States v. Auernheimer, No. 11-CR-470 SDW.

[48] *See id*.

[49] *See* Superseding Indictment, *supra* note 44, at 1–15.

[50] *See* Verdict, United States v. Auernheimer, No. 11-CR-470 SDW (D.N.J. Nov. 20, 2012), 2012 WL 6676886.

[51] *See* United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2013).

[52] U.S. v. Auernheimer, ELEC. FRONTIER FOUND., https://www.eff.org/cases/us-v-auernheimer (last visited Aug. 23, 2014); USA v. Andrew Auernheimer *Docket Report*, JUSTIA, http://dockets.justia.com/docket/circuit-courts/ca3/13-1816 (last visited Aug. 23, 2014).

[53] *See* Superseding Indictment, *supra* note 44.

[54] Brief of Amicus Curiae Digital Media Law Project in Support of Defendant–Appellant at 26, United States v. Auernheimer, No. 13-1816 (3d Cir. 2013), 2013 WL 3488592.

[55] *See id.* at 32.

> heavy-handed and chilling applications of law to set the ethical norms around this delicate and complicated space.[56]

¶19 The Government's reply, in contrast, attempted to draw a line for appropriate data-vulnerability disclosure;[57] specifically, that the content divulged, rather than the act itself, dictated the legality of Auernheimer's disclosure.[58] Though its brief conceded that Auernheimer could have legally reported AT&T's vulnerability, the Government asserted, "What he could not do, and what is not subject to First Amendment protection, is disclose the personal identifying information that he and Spitler obtained as a result of their breach of AT&T's security."[59] In short, the Government argued that Auernheimer and Spitler acted illegally due to the disclosure of personal information, which is not protected speech.

¶20 But the Third Circuit Court of Appeals chose to focus on venue, foregoing the opportunity to address vulnerability-speech protection.[60] The court found that no essential conduct element of the crime occurred in New Jersey, despite Auernheimer having exposed information from New Jersey residents. "As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue," wrote Judge Chagares.[61] Pointing to the fact that Auernheimer and Spitler resided in Arkansas and California, respectively, and that AT&T's servers were based in Georgia and Texas, the court found the connection to New Jersey insufficient to support venue.[62]

¶21 Auernheimer's release, however, did not preclude authorities in an appropriate venue from pursuing prosecution. The risk of a court reviewing disclosure policies and endorsing a single model, as was possible in this case, illustrates the possibility of judicial intervention in determining vulnerability-speech policy. Although balancing First Amendment interests is within the purview of the judiciary, this still-evolving and highly-technical landscape requires authoritative restraint for healthy debate amongst the data security community and the public alike to work effectively, guiding the contours, at least initially, of vulnerability-speech protection.

C. The First Amendment and the Prior Restraint Doctrine

¶22 Any preemptive restriction on protected speech, which a responsible disclosure policy engenders, implicates the "doctrine of prior restraint." A prior restraint is an official restriction delaying or prohibiting speech in advance of actual publication. "In constitutional terms, the doctrine of prior restraint holds that the First Amendment forbids the Federal Government to impose any system of prior restraint, with certain limited

---

[56] *Id.* at 31 (internal citations omitted).
[57] Brief for Appellee, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2013) (No. 13-1816).
[58] *See id.* at 121.
[59] *Id.*
[60] *See* Oral Argument, United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2013) (No. 13-1816), *available at* http://www2.ca3.uscourts.gov/oralargument/audio/13-1816USAv.Auernheimer.wma; *Auernheimer*, 748 F.3d 525; *see also* Brian Merchant, *Weev Is in Jail Because the Government Doesn't Know What Hacking Is*, MOTHERBOARD (Mar. 19, 2014, 3:25 PM), http://motherboard.vice.com/read/weev-is-in-jail-because-the-government-doesnt-know-what-hacking-is.
[61] *Auernheimer*, 748 F.3d at 541.
[62] *See id*.

exceptions, in any area of expression that is within the boundaries of that Amendment," wrote Professor Thomas Emerson, summarizing the prior restraint doctrine.[63] Stated differently, blanket preventative measures aimed to restrict protected speech before publication conflict with First Amendment rights, unless a judicial exception applies.

¶23 The convention of disfavoring prior restraints has been a primary tenet of Anglo-American law for most of modern history. In response to licensing schemes designed to control printing,[64] Sir William Blackstone perhaps best articulated the early distaste for prior restraints:

> The liberty of the press is indeed essential to the nature of a free state; but this consists in laying no previous restraints upon publications, and not in freedom from censure for criminal matter when published. Every freeman has an undoubted right to lay what sentiments he pleases before the public; to forbid this, is to destroy the freedom of the press; but if he publishes what is improper, mischievous or illegal, he must take the consequence of his own temerity.[65]

The Framers of the U.S. Constitution evinced a sentiment similar to Blackstone's antipathy for prior restraints.[66] In fact, the founding fathers extended the reach of this doctrine beyond its English counterpart. Opining on the Sedition Act and freedom of the press, James Madison wrote, "This security of the freedom of the press requires that it should be exempt not only from previous restraint by the Executive, as in Great Britain, but from legislative restraint also."[67] Madison recognized that in order to protect freedom of the press effectively, the First Amendment must apply equally to all branches of the government.

¶24 In the twentieth century, the U.S. Supreme Court revitalized the prior restraint doctrine, expanding the scope of First Amendment protection. The Court recognized that the First Amendment's primary purpose is "to prevent all such previous restraints upon publications as had been practiced by other governments,"[68] forming the basis for the doctrine's revival in the influential prior restraint case *Near v. Minnesota*.[69] In that case, a Minnesota court had enjoined a weekly newspaper from issuing "any publication

---

[63] Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 LAW & CONTEMP. PROBS. 648, 648 (1955). These limitations are applied to the states via Fourteenth Amendment incorporation. For a more detailed and nuanced discussion of the doctrine of prior restraint, see Stephen R. Barnett, *The Puzzle of Prior Restraint*, 29 STAN. L. REV. 539 (1977); Vincent Blasi, *Toward a Theory of Prior Restraint: The Central Linkage*, 66 MINN. L. REV. 171 (1981); John C. Jeffries, *Rethinking Prior Restraint*, 92 YALE L.J. 409 (1983); Martin H. Redish, *The Proper Role of the Prior Restraint Doctrine in First Amendment Theory*, 70 VA. L. REV. 53 (1984); Jeffery A. Smith, *Prior Restraint: Original Intentions and Modern Interpretations*, 28 WM. & MARY L. REV. 439 (1987).

[64] *See* Emerson, *supra* note 63, at 650–52.

[65] 4 WILLIAM BLACKSTONE, COMMENTARIES *151–52.

[66] U.S. CONST. amend. I.

[67] James Madison, *Report on the Virginia Resolutions in* 6 WRITINGS OF JAMES MADISON 385, 387 (Gaillard Hunt ed. 1900), *available at* http://press-pubs.uchicago.edu/founders/documents/amendI_speechs24.html. He went on to describe the understanding at the Constitutional Convention as being "that the liberty of conscience and the freedom of the press were equally and completely exempted from all authority whatever of the United States." *Id.*

[68] Patterson v. Colorado *ex rel.* Att'y Gen., 205 U.S. 454, 462 (1907).

[69] Near v. Minnesota, 283 U.S. 697 (1931).

whatsoever which is a malicious, scandalous or defamatory newspaper, as defined by law."[70] The Supreme Court recognized this "effective censorship" as an unconstitutional prior restraint and vacated the injunction, noting the Framers' clear opposition to government-sanctioned prepublication restrictions:

> The exceptional nature of its limitations places in a strong light the general conception that liberty of the press, historically considered and taken up by the Federal Constitution, has meant, principally although not exclusively, immunity from previous restraints or censorship.[71]

¶25 The presumption against prior restraints remains salient despite the exceptions and limitations to this doctrine discussed *infra* Part III.[72] Decades after its holding in *Near*, the Court affirmed that "prior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights."[73] Part III discusses the implications of the prior restraint doctrine on potential government regulation addressing data vulnerability disclosures.

III. PRIOR RESTRAINT APPLICATION

A. Responsible Disclosure as a Prior Restraint

¶26 "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."[74] The Court endorsed the broad application of this doctrine in *Near v. Minnesota*,[75] presuming the unconstitutionality of prepublication censorship imposed by state law. A government-compelled mechanism requiring responsible disclosure (e.g., mandatory disclosure to a company before public dissemination) would thus obligate the government to rebut this presumption if the policy restrained protected speech.

¶27 Proponents of the responsible disclosure approach point to the potential for abuse in a full disclosure system to counter constitutional deficiencies.[76] For instance, disclosing a data vulnerability might inspire "blackhat" hackers to exploit the weakness before a data-holder is able to resolve the threat.[77] Alternatively, a party wishing to gain an unfair advantage over a competitor might anonymously report a data breach, resulting in reputational damage and decreased user-traffic for the affected data-holder, regardless

---

[70] *Id.* at 703.
[71] *Id.* at 716.
[72] *See infra* Part III(B).
[73] Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).
[74] *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963); *see also Neb. Press Ass'n*, 427 U.S. at 592; Heller v. New York, 413 U.S. 483, 491 (1973); N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971); Freedman v. Maryland, 380 U.S. 51, 57 (1965).
[75] 283 U.S. 697 (1931).
[76] *See* ALANA MAURUSHAT, DISCLOSURE OF SECURITY VULNERABILITIES: LEGAL AND ETHICAL ISSUES (2013) (outlining the disclosure debate and problems with full disclosure).
[77] Jonathan Trull, *Responsible Disclosure: Cyber Security Ethics*, CSO (Feb. 26, 2015, 5:27 AM), http://www.csoonline.com/article/2889357/security0/responsible-disclosure-cyber-security-ethics.html ("The argument for responsible disclosure is that blackhats—cyber criminals—can typically exploit the vulnerability when publicly disclosed much quicker than those who are attacked can fix the issue.").

of the disclosure's veracity. Yet, while this potential for unlawful abuse prompts some concerns, the mere possibility of exploitative conduct does not justify quashing First Amendment rights: "The fact that the liberty of the press may be abused by miscreant purveyors of scandal does not make any the less necessary the immunity of the press from previous restraint."[78] In short, the presence of a few bad actors should not compel the preemptive restriction of constitutionally protected speech. And although punishment following public disclosure might be constitutionally sound in certain instances, the possibility of future legal recourse does not alleviate a prior restraint regime's inherent constitutional infirmity.[79]

¶28 Furthermore, the fact that a policy might allow the publication of a data weakness following a company's resolution thereof does not rectify these constitutional issues. Delay, not just outright prohibition of publication, may constitute a prior restraint. For example, the Supreme Court in *Nebraska Press Association v. Stuart* struck down a court order restricting pretrial reporting of confessions in a popular murder trial.[80] The Court noted:

> The order at issue . . . does not prohibit but only postpones publication. Some news can be delayed and most commentary can even more readily be delayed without serious injury, and there often is a self-imposed delay when responsible editors call for verification of information. But such delays are normally slight and they are self-imposed. Delays imposed by governmental authority are a different matter.[81]

In reaching its holding, the Court focused not on the content of the publication but on the potential damage caused by a delay and its source—the government—in determining that the court order violated First Amendment rights.

¶29 Government-imposed delays are a "different matter" because they are neither "slight" nor "self-imposed."[82] Like any other impermissible restraint, what makes this type of censorship unconstitutional is its impact on free speech. More precisely, the adverse effects of a lengthy delay (e.g., the extent of potential harm) and the degree of free speech quashed (e.g., the amount of editorial discretion stymied) determine the restriction's constitutionality. Accordingly, with regard to prepublication censorship, the greater the amount of harm caused and speech-discretion stifled, the more likely the restraint violates First Amendment rights.

¶30 Addressing these factors in the data security context, a government-imposed publication delay should be analogously impermissible. In fact, the likely effects of a responsible disclosure policy suggest it would be even less constitutionally sound than the court order struck down in *Nebraska Press*. In data security cases, for instance, delaying news of a data vulnerability could significantly alter the initially intended message and its corresponding importance. While the consequences of disclosure might

---

[78] 283 U.S. at 720.

[79] *See id*. ("Subsequent punishment for such abuses as may exist is the appropriate remedy, consistent with constitutional privilege.").

[80] *See* 427 U.S. 539.

[81] *Id*. at 560.

[82] *Id.*

be uncertain initially, delay poses a risk of serious injury to those whose data is exposed—an injury that can be substantially mitigated, if not altogether avoided, if notice of a breach is provided without delay. Moreover, individual security researchers or news editors may choose to delay publication, for example, when they believe publication might violate privacy rights or a source's credibility needs confirmation. Companies may also provide incentives for those who discover vulnerabilities to delay disclosure.[83] Coupled with the potential for widespread harm, the amount of discretion stifled—namely the various alternatives to public disclosure—prompts serious constitutional concerns for any responsible disclosure policy.

¶31 In addition, the special character of the press and the role it plays in society highlights why even short delays in publication can have pernicious consequences. As society adapts to a twenty-four-hour news cycle, the expectation of timeliness has never been more prominent: "As a practical matter, moreover, the element of time is not unimportant if press coverage is to fulfill its traditional function of bringing news to the public promptly."[84] Though immediate access to a news story may have been impossible when news came only in the form of a daily paper, the advent of the Internet demands immediate reporting. News outlets that fail to adapt to this rapid news cycle will likely lose readers because consumers do not expect to wait for news of any significance.[85] And as discussed previously, immediacy is of particular importance with respect to data security because punctual reporting allows consumers to take cautionary steps to protect their personal information, with even the slightest delay potentially resulting in mass exploitation of consumer data.

¶32 Nevertheless, the presumption against prior restraints is not absolute. A more complete understanding of the constitutionality of a government-endorsed vulnerability disclosure policy requires consideration of the value of the speech protected and the government's interests in delaying disclosure.

B. Protecting Vulnerability Speech

¶33 The First Amendment provides more protection for ex ante speech than ex post speech. As the Supreme Court recognized in *Nebraska Press*, "The First Amendment . . . accords greater protection against prior restraints than it does against subsequent punishment for a particular speech."[86] The reason for this temporal distinction finds itself in the fundamental principle that censoring free speech discourages the development and protection of a marketplace of ideas:

> [A] free society prefers to punish the few who abuse rights of speech after they break the law than to throttle them and all others beforehand. It is always difficult to know in advance what an individual will say, and the

[83] *See supra* notes 161–66 and accompanying text.

[84] *Neb. Press Ass'n*, 427 U.S. at 561.

[85] *See, e.g.,* Liane Hansen & David Folkenflik, *The Power of the 24-Hour News Cycle*, NAT'L PUB. RADIO (May 29, 2005, 12:00 AM), http://www.npr.org/templates/story/story.php?storyId=4671485.

[86] *Neb. Press Ass'n*, 427 U.S. at 589 (citing Carroll v. Princess Anne, 393 U.S. 175, 180–81 (1968)).

> line between legitimate and illegitimate speech is often so finely drawn that the risks of freewheeling censorship are formidable.[87]

Determining the extent of First Amendment protection for after-the-fact vulnerability speech requires fact-specific, case-by-case analysis and not a restrictive, prophylactic responsible-disclosure mandate.

¶34 Because of this aversion to censorship, courts may consider the context of the disclosure and the motivation of the parties involved in determining the extent of First Amendment protection. Pertinent to data vulnerability disclosures, this context-based approach provides guidance in determining the level of constitutional protection for the dissemination of computer code or, more precisely, whether computer code constitutes protected speech under the First Amendment and how far this protection might extend.[88] The Fourth Circuit Court of Appeals illustrated this approach in *Ostergen v. Cuccinelli*, where it held that First Amendment protection extended to the disclosure of social security numbers because the disclosure was meant to convey a message about the inappropriateness of the state's treatment of documents containing private information.[89] While disclosing social security numbers is not itself protected speech, the context elevated the otherwise unprotected speech content to protected expression.

¶35 Thus, under the reasoning of *Ostergen*, even if code alone is not protected speech, various situations could similarly elevate the disclosure of computer code to allow First Amendment protection. Computer code, for instance, can be integral to conveying the veracity and importance of resolving data security vulnerabilities.[90] Keeping this in mind, disseminated code more likely comprises protected speech in scenarios with the most pervasive and complex data exposures. Accordingly, as the potential damage of a data breach increases, the necessity of computer code also increases, supporting the extension of First Amendment protection following dissemination. Yet the most significant takeaway from employing this context-based approach goes far beyond its application to computer code. Indeed, it is simply the fact that computer code—in its perfunctory and mechanical form—can amount to protected speech even after publication that is critical, granting further constitutional vindication for vulnerability-speech protection.

¶36 Most importantly, data security is a matter of public concern, which makes the potential harm caused by prior restraints and delays more salient. The Supreme Court

---

[87] Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 559 (1975).

[88] Courts and scholars alike have been reasoning through this debate. *See, e.g.,* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); Junger v. Daley, 209 F.3d 481 (6th Cir. 2000); Bernstein v. U.S. Dep't of Justice, 192 F.3d 1308 (9th Cir. 1999); *see also* Dan Burk, *Patenting Speech*, 79 TEX. L. REV. 99 (2000); Orin Kerr, *Are We Overprotecting Code?: Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287 (2000); Ethan Preston & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability, and the First Amendment*, 24 WHITTIER L. REV. 71 (2002); Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629 (2000). Though a compelling issue, this Article will not thoroughly address the role of code in vulnerability speech and the implications it may have on First Amendment protection and analysis. This debate need not be resolved in order to decide whether First Amendment protection against prior restraints may extend to vulnerability speech that incorporates code.

[89] *See generally* Ostergen v. Cuccinelli, 615 F.3d 263 (4th Cir. 2010).

[90] *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS 228 (2006) (recognizing that news reporting online is most effective when the "[t]he first move . . . is to make the raw materials available for all to see").

recognized the need to account for the public interest in prior restraint cases, specifically acknowledging in *Nebraska Press* that "[t]he damage can be particularly great when the prior restraint falls upon the communication of news and commentary on current events."[91] In addition to contemporaneousness, speech constitutes a matter of public concern when it relates to political, social, or community issues.[92] It is difficult to imagine that data security information fails to qualify as a matter of public concern of the type contemplated by the Court.

¶37 Empirical evidence supports this argument, showing that most modern consumers fear the loss of personal information through a data breach. Even before Target's data breach personally affected millions of consumers, concern over the security of personal data was endemic. For example, a survey conducted in March 2013 revealed that 82.1% of Americans were at least somewhat worried about a data breach involving banks, government entities, or other organizations, and roughly the same percentage were concerned about identity theft and credit-card fraud.[93] This wariness remains significant. Since the breach at Target—and breaches at many other retailers—over half of those surveyed said that an actual security breach would make them less likely to do business with the bank or store breached.[94] And with over 78-million data records containing personal information exposed to breaches in the first ten months of 2014 alone, it is unsurprising that a separate survey found that 77% of consumers agreed that prompt notification of vulnerabilities involving stolen or lost data was important.[95] Because of this fear, state legislatures—typically the primary enactors of consumer-protection laws—have passed various data-breach-notification statutes, requiring companies to inform customers of significant security breaches involving personal information, which reinforces the stance that protecting private information and promoting mitigation upon breach is irrefutably a matter of public concern.[96]

¶38 State legislatures are not alone. The Executive branch has recognized the broader importance of cybersecurity, instating a National Cybersecurity Initiative and identifying "cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[97] Before the 2015 State of the Union address, President Obama

---

[91] *Neb. Press Ass'n*, 427 U.S. at 559.

[92] *See* Snyder v. Phelps, 131 S. Ct. 1207, 1211 (2011) ("Although the boundaries of what constitutes speech on matters of public concern are not well defined, this Court has said that speech is of public concern when it can 'be fairly considered as relating to any matter of political, social, or other concern to the community,' or when it 'is a subject of general interest and of value and concern to the public.'") (internal citations omitted).

[93] LIEBERMAN RESEARCH GRP., UNISYS SECURITY INDEX: US, UNISYS (Apr. 18, 2013), *available at* http://www.unisyssecurityindex.com/system/reports/uploads/288/original/Unisys%20Security%20Index_United%20States_May%202013.pdf?1370347491.

[94] LIEBERMAN RESEARCH GRP., UNISYS SECURITY INDEX: US, UNISYS (May 13, 2014), *available at* http://www.unisyssecurityindex.com/system/reports/uploads/303/original/Unisys%20Security%20Index%20US%20May%202014.pdf?1399929399.

[95] EMC CORP., *supra* note 12.

[96] *See* MINTZ LEVIN, STATE DATA SECURITY BREACH NOTIFICATION LAWS (Jan. 1, 2015), *available at* http://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf (providing a chart of state-enacted notification laws).

[97] *The Comprehensive National Cybersecurity Initiative*, WHITE HOUSE, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (last visited Mar. 18, 2014).

reaffirmed his administration's commitment to cybersecurity and detailed various proposals to combat cyber threats, including a proposal for a federal data-breach-notification law.[98] Though data vulnerabilities and corporate responsibility constitute a small sliver of a larger cybersecurity problem, the disclosure issue nevertheless remains a prominent, unresolved challenge.

C. Permissible Prior Restraints

¶39 Although the presumption against prior restraints is strong, it is not absolute. The Supreme Court has recognized limitations to the prior restraint doctrine that permit prepublication restrictions on speech. However, qualifying for an exception requires meeting a high evidentiary threshold: the Government "carries a heavy burden of showing justification for the imposition of . . . a [prior] restraint,"[99] and the recognized exceptions are "extremely difficult to justify."[100] Although some danger may be posed by the publication of information about a data vulnerability, this Article posits that any formal adoption of a responsible disclosure policy invariably fails to meet this heavy burden.

¶40 The Supreme Court in *Near v. Minnesota* held that an injunction against a newspaper for exposing illicit activities of state politicians constituted an unconstitutional prior restraint.[101] In dicta, however, the Court acknowledged that prior restraints might be appropriate in limited circumstances:

> [T]he protection even as to previous restraint is not absolutely unlimited. But the limitation has been recognized only in exceptional cases. "When a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right." No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops. On similar grounds, the primary requirements of decency may be enforced against obscene publications. The security of the community life may be protected against incitements to acts of violence and the overthrow by force of orderly government.[102]

Of particular relevance to vulnerability speech is the "national-security exception" *Near* identifies, also referred to as the "military-security exception," which permits prior restraints when there is an immediate risk to national security.

¶41 Two cases—*New York Times Co. v. United States*[103] and *United States v. Progressive*[104]—illustrate the extraordinary circumstances necessary to meet the national-

[98] *Safeguarding American Consumers & Families*, *supra* note 16.

[99] Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971); *see also* N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971).

[100] Neb. Press Ass'n v. Stuart, 427 U.S. 539, 592 (1976).

[101] *See* Near v. Minnesota, 283 U.S. 697 (1931).

[102] *Id.* at 716 (quoting Schenck v. United States, 249 U.S. 47, 52 (1919)).

[103] 403 U.S. 713 (1971).

security exception for prior restraints. In *New York Times Co.*, the Supreme Court reviewed the Government's motion for an injunction against the *New York Times* and the *Washington Post* preventing publication of the "Pentagon Papers," which included classified details about the United States' involvement in Vietnam.[105] Though there was no majority opinion, a per curiam opinion declared that the Government had not met its "heavy burden" of justifying a prior restraint,[106] notwithstanding the fact that a majority of Justices acknowledged that the release of the top-secret documents would in fact harm national security—some even noting that the newspapers might face prosecution after publication under various espionage statutes.[107] Even after recognizing this harm, the Court refused to permit a prior restraint. Of the six Justices who authored concurrences, two asserted that First Amendment protection absolutely precludes prior restraints,[108] while the remaining four construed the national-security exception narrowly.[109]

¶42 Less than a decade after the Supreme Court decided *New York Times Co.*, the national-security exception was successfully raised in a U.S. District Court in Wisconsin.[110] Amidst the height of the Cold War, the district court reviewed an injunction under the Atomic Energy Act that prevented the *Progressive* from publishing a "how to" article on building a hydrogen bomb.[111] Recognizing that "few things, save grave national security concerns, are sufficient to override First Amendment interests," the court enjoined the defendant from publishing the article[112] because it provided sufficient information for a nation to expedite its development of a hydrogen bomb and provided little value to any public debate over atomic weapons.[113] Unlike the Pentagon Papers, this publication contained contemporary information that could affect the nation's security during wartime.[114] Relying on the Supreme Court's military-security language in *Near*, the district court concluded that "publication of the technical information on the hydrogen bomb contained in the article is analogous to publication of troop movements or locations in time of war and falls within the extremely narrow exception to the rule against prior restraint."[115] Drawing specifically from Justice Stewart's concurrence in

---

[104] 467 F. Supp. 990 (W.D. Wis. 1979).

[105] *See* 403 U.S. 713.

[106] *Id*. at 714.

[107] *See id*. at 720–24 (Douglas, J., concurring); *id*. at 730–40 (White, J., concurring); *id*. at 740–48 (Marshall, J., concurring); *id*. at 748–52 (Burger, J., dissenting); *id*. at 759–62 (Blackmun, J., dissenting); Neb. Press Ass'n v. Stuart, 427 U.S. 539, 591–92 (1976).

[108] *See N.Y. Times Co.*, 403 U.S. at 714–20 (Black, J., concurring); *id*. at 720–24 (Douglas, J., concurring).

[109] *See id*. at 724–27 (Brennan, J., concurring) ("[G]overnmental allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea . . . . [But] [i]n no event may mere conclusions be sufficient."); *id*. at 727–30 (Stewart, J., concurring) (requiring "direct, immediate, and irreparable damage to our Nation or its people"); *id*. at 730–40 (White, J., concurring) (recognizing that even demonstrating that "revelation of these documents will do substantial damage to public interests" is insufficient to overcome the "extraordinary protection against prior restraints"); *id*. at 740–48 (Marshall, J., concurring).

[110] *See* United States v. Progressive, 467 F. Supp. 990 (W.D. Wis. 1979).

[111] *See id*.

[112] *See id*. at 992, 997.

[113] *See id*. at 993–94. "A mistake in ruling against the United States could pave the way for thermonuclear annihilation for us all. In that event, our right to life is extinguished and the right to publish becomes moot." *Id*. at 996.

[114] *See id*. at 994.

[115] *Id*. at 996.

New York Times Co.,[116] the court asserted that the United States met its burden of demonstrating grave, immediate harm to the nation.

¶43 Though little guidance exists for how to balance national security interests with freedom of the press, disclosure of data vulnerabilities unlikely poses a sufficiently significant threat to national security for the Government to meet this heavy burden. Crucially, data vulnerabilities are primarily a matter of concern between consumers and retailers or financial institutions. The exploitation of a vulnerability most often implicates consumer-data privacy and company reputations, not national security. With this in mind, the Supreme Court has noted on numerous occasions that the invasion of privacy is insufficient to support an injunction against the press.[117] The fact that the majority of data breaches threaten privacy rights rather than U.S.-state interests—let alone national security interests—makes justifying any government-imposed preventative measures incredibly difficult. Furthermore, the severity of harm resulting from the revelation of a data vulnerability is far less than that presented by instructions on composing an atomic bomb. To be sure, the damage that could result from the exploitation of data—fraud and identity theft likely being the most extreme—pales in comparison to the substantial loss of life that could result from nuclear proliferation. In this same vein, but to a lesser degree, the revelation of former military strategies in the Pentagon Papers posed a more grave, immediate, and irreparable harm than consumer fraud.

¶44 Yet, while data security breaches are predominantly a concern for consumers, the U.S. government and state governments are similarly susceptible. For example, in the first few months of 2014 alone, the U.S. Veterans of Foreign Wars website was hacked,[118] California's Department of Motor Vehicles online credit-card database was breached,[119] data tables on several government websites were manipulated,[120] and a bug shut down PACER.[121] Government websites, like any other, are vulnerable to exploitation.

¶45 But government-website data breaches that implicate national security are rare.[122] In light of this realistic infrequency, legislation concerning vulnerability speech would

[116] *See* N.Y. Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., concurring) ("But I cannot say that disclosure of any of them will surely result in direct, immediate, and irreparable damage to our Nation or its people.").

[117] *See, e.g.,* Bartnicki v. Vopper, 532 U.S. 514 (2001); Neb. Press Ass'n v. Stuart, 427 U.S. 539, 558 (1976); Org. for a Better Austin v. Keefe, 402 U.S. 415, 418–20 (1971); *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214 (1890–91) ("The right of privacy does not prohibit any publication of matter which is of public or general interest.").

[118] Kristin Bergman, *Hackers Take Aim at Veterans That Use Internet Explorer*, IT-LEX (Feb. 24, 2014), http://it-lex.org/hackers-take-aim-at-veterans-that-use-internet-explorer/.

[119] Kate Mather & Carla Rivera, *Possible Breach of DMV Online Customers' Credit Card Data Reported*, L.A. TIMES (Mar. 22, 2014, 12:34 PM), http://www.latimes.com/local/lanow/la-me-ln-california-dmv-breach-20140322,0,5390096.story#axzz2wkDWoEiq.

[120] Jeryl Bier, *Opportunistic Marketers Exploit Opening at Healthcare.gov*, WKLY. STANDARD (Jan. 23, 2014, 7:04 AM), http://www.weeklystandard.com/blogs/opportunistic-marketers-exploit-opening-healthcaregov_775259.html; Jeryl Bier, *Widespread Vulnerability Found in Dozens of Government "Open Data" Websites*, WKLY. STANDARD (Feb. 20, 2014, 8:07 AM), https://www.weeklystandard.com/blogs/widespread-vulnerability-found-dozens-government-open-data-websites_782700.html.

[121] Devlin Barrett, *FBI: Glitches, Not Cyberattack, Disrupted Court Websites*, WALL ST. J. (Jan. 24, 2014, 11:25 PM), http://online.wsj.com/news/articles/SB10001424052702303448204579341523348986810.

[122] Take, for example, data breaches in 2014. At the end of the year and in early 2015, dozens of

likely implicate the First Amendment's "overbreadth doctrine." The overbreadth doctrine "is an exception to the established principle that 'a person to whom a statute may constitutionally be applied will not be heard to challenge that statute on the ground that it may conceivably be applied unconstitutionally to others, in other situations not before the Court.'"[123] Thus, even a defendant whose speech or activities fall outside First Amendment protection may challenge a law's constitutionality when "the possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted."[124] But for a facial challenge to the validity of an entire statute to succeed, its overbreadth "must not only be real but substantial as well, judged in relation to the statute's plainly legitimate sweep."[125] Thus, while a vulnerability may threaten national security to such a degree that it satisfies the military-security exception, the vast amount of protected speech "muted" by responsible disclosure legislation likely precludes the constitutionality of such a heavy-handed approach.[126] Stated differently, this type of legislation's over-inclusiveness would be both real and substantial, stifling myriad instances of protected speech while only minimally benefitting national security.

¶46 Rather than legislating a general vulnerability policy, these extreme scenarios should be resolved in a less restrictive manner. This may involve case-by-case determinations requiring fact-specific analyses or narrowly-tailored legislation regulating disclosure of vulnerabilities in government computer systems. Adopting a responsible disclosure policy for all data security vulnerabilities is not an appropriately tailored response for the limited circumstances that might qualify for the national-security exception.

D. Procedural Requirements

¶47 In addition to these substantive challenges, any legislation mandating a responsible disclosure policy would need to satisfy the procedural requirements established in

---

organizations expounded upon what they considered the most significant breaches. Notably, very few of these breaches implicated national security, and arguably none reached the severity required to satisfy the national-security exception to the prior restraint doctrine. *See, e.g.,* Bitium, *The Biggest Data Breaches and Hacks of 2014*, RE/CODE (Feb. 10, 2015, 12:05 PM), http://recode.net/2015/02/10/the-biggest-data-breaches-and-hacks-of-2014/; Khidr Suleman, *Biggest Hacks of 2014: From Apple to eBay, No-One Is Safe*, ITPRO (Dec. 8, 2014), http://www.itpro.co.uk/security/23673/biggest-hacks-of-2014-from-apple-to-ebay-no-one-is-safe; Zack Whittaker, *2014 In Security: The Biggest Hacks, Leaks, and Data Breaches*, ZDNET (Dec. 28, 2014, 6:32 PM), http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches/. Even the seemingly dangerous hack of U.S. Central Command's Twitter feed by ISIS sympathizers was just that—a social media account hack resulting in fear and embarrassment, not a breach of intelligence information. The Twitter account's vulnerability was exploited for what CENTCOM called "cybervandalism"; there was no risk of exposure of classified information by the hack. *See* Dan Lamothe, *U.S. Military Social Media Accounts Apparently Hacked by Islamic State Sympathizers*, WASH. POST (Jan. 13, 2015, 12:53 PM), http://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/.

[123] R.A.V. v. City of St. Paul, Minn., 505 U.S. 377, 412 (1992) (citing Broaderick v. Oklahoma, 413 U.S. 601, 610 (1973)).

[124] *Broaderick*, 413 U.S. at 612.

[125] *Id.* at 615.

[126] Indeed, an early 2015 hack of U.S. Central Command's Twitter account hints at the type of vulnerability that may satisfy this exception. Paul D. Shinkman, *U.S. Central Command Twitter Account Suspended After Apparent ISIS Hack*, U.S. NEWS (Jan. 12, 2015, 2:06 PM), http://www.usnews.com/news/articles/2015/01/12/us-central-command-twitter-account-suspended-after-apparent-isis-hack.

Freedman v. Maryland.[127] In *Freedman*, the Supreme Court struck down a state law that required censors to approve films before allowing them in theatres, aiming to screen out films that were obscene or likely to incite crime.[128] Analogously, a responsible disclosure policy requires a review process mandating "submission" to the affected company, which in turn obligates the would-be discloser to refrain from publishing his findings until either a predetermined amount of time elapses or the company approves.[129]

¶48 *Freedman* set forth four procedural requirements for any such censoring system to survive First Amendment scrutiny. The Court held that "a noncriminal process which requires the prior submission of a film to a censor avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system."[130] The Court went on to outline these safeguards:

> First, the burden of proving that the film is unprotected expression must rest on the censor. . . . Second, while the State may require advance submission . . . the requirement cannot be administered in a manner which would lend an effect of finality to the censor's determination whether a film constitutes protected expression. . . . [O]nly a procedure requiring a judicial determination suffices to impose a valid final restraint. . . . [Third,] the exhibitor must be assured, by statute or authoritative judicial construction, that the censor will, within a specified brief period, either issue a license or go to court to restrain showing the film . . . and must similarly be limited to preservation of the status quo for the shortest fixed period compatible with sound judicial resolution. . . . [Fourth,] the procedure must also assure a prompt final judicial decision, to minimize the deterrent effect of an interim and possibly erroneous denial of a license.[131]

These procedural safeguards must be in place for any prior-submission form of censorship to survive First Amendment scrutiny.[132]

¶49 Moreover, in the context of vulnerability disclosures, many commercial incentives exist making a responsible disclosure policy ripe for abuse, increasing the necessity of these procedural safeguards. For instance, facing potential embarrassment and reputational damage resulting from the revelation of a vulnerability, data-holders may feel threatened by external data-security inspections. Fearing exposure of data security deficiencies, companies may not cooperate with security experts or, worse yet, refuse to acknowledge clear security defects following an inspection. And, now more than ever, successful directors and corporate executives are often measured not by long-term growth but by recent share prices, increasing the temptation to conceal data weaknesses from the

---

[127] Freedman v. Maryland, 380 U.S. 51 (1965).
[128] *See id*.
[129] *See* ORG. FOR INTERNET SAFETY, *supra* note 22.
[130] *Freedman,* 380 U.S. at 58.
[131] *Id.* at 58–60.
[132] *Id.* at 57–58 ("Because the censor's business is to censor, there inheres the danger that he may well be less responsive than a court—part of an independent branch of government—to the constitutionally protected interests in free expression. And if it is made unduly onerous, by reason of delay or otherwise, to seek judicial review, the censor's determination may in practice be final.").

public and avoid confronting any shortcomings head-on.[133] Thus, although companies often understandably wish to prevent the publication of data security weaknesses, misaligned interests coupled with the ability to conceal institutional flaws increase the potential for unchecked abuse, further bolstering the need for procedural safeguards in the data security context.

¶50 Therefore, even if Congress were to draft a responsible disclosure bill sufficiently tailored to pass substantive constitutional review, Congress would still need to put in place adequate procedural safeguards. Specifically, the legislation must include provisions that: (1) place the burden on the data-holder to show the disclosure implicates unprotected expression; (2) ensure the data-holder's decision does not "lend an effect of finality"; (3) limit the delay to a brief period; and (4) provide for expedited judicial review.[134]

IV. EDITORIAL PROTECTIONS OF THE PRESS

¶51 As desirable as it may seem, mandating a privacy-conscious press is antithetical to First Amendment principles. Notwithstanding certain exceptional circumstances, courts must not interfere with editorial discretion to force responsible newsgathering and publication. "Bad conduct never justifies prior restraint," and "the Supreme Court has held consistently to the view that newsgathering conduct by itself never justifies enjoining publication."[135] Regardless of the means by which a third party procured information, if the press obtains this information through lawful newsgathering, First Amendment protection applies.[136] Thus, even if a policy applies only to vulnerability information that a source obtained illegally, a policy preventing publication of this information would impermissibly restrain freedom of the press.

¶52 The principle that a source's conduct should not affect the press's right to disseminate remains salient. The Court first articulated this in *Bartnicki v. Vopper*,[137] where a local radio station anonymously received an illegally recorded discussion between a union president and chief negotiator.[138] The Court refused to enjoin the

---

[133] *See* Leo Strine, Jr., *One Fundamental Corporate Governance Question We Face: Can Corporations Be Managed for the Long Term Unless Their Powerful Electorates also Act and Think Long Term?*, BUS. LAW., Nov. 2010, at 1, 16 ("[I]f the electorate . . . does not push an agenda that appropriately focuses on the long term, the responsiveness of managers to the incentives they face can result in business strategies that involve excessive risk . . . ."); *see also* Dominick Barton & Mark Wiseman, *Where Boards Fall Short*, HARV. BUS. REV., Jan.–Feb. 2015.

[134] *See Freedman,* 380 U.S. at 58–60.

[135] Robert M. O'Neil, *Tainted Sources: First Amendment Rights and Journalistic Wrongs*, 4 WM. & MARY BILL RTS. J. 1005, 1024 (1996).

[136] *See* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) ("[A] stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern.").

[137] *See id*.

[138] *Id*. Analogous to the intersection of data security and vulnerability speech, the Court began by recognizing the conflict posed by evolving technology:

> [T]hese cases present a conflict between interests of the highest order—on the one hand, the interest in the full and free dissemination of information concerning public issues, and, on the other hand, the interest in individual privacy. . . . The Framers of the First Amendment surely did not foresee the advances in science that produced the conversation, the interception, or the conflict that gave rise to this action.

publication, stating, "[A] stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern."[139] Specifically, the Court highlighted three factors in making this decision: (1) the press had no role in the illegal interception; (2) the press obtained access to the recording lawfully; and (3) the recording depicted a matter of public concern.[140] Applying *Bartnicki* to a typical vulnerability-disclosure scenario, a news outlet would meet the first two factors by showing that a security researcher, acting legally or illegally, uncovered a data weakness and conveyed this information to a member of the press on the security researcher's own prerogative. As for the third factor, information about data security breaches often implicates millions of consumers,[141] undoubtedly fulfilling the public-concern inquiry articulated in *Bartnicki*, which involved collective-bargaining negotiations between a local schoolboard and a teacher's union.[142] Therefore, in the most likely vulnerability-disclosure scenario, neither the press's right to publish nor the government's interest in imposing a prior restraint are affected by a source's wrongful conduct.[143]

¶53 Beyond these constitutional issues, governmental interference prompts credibility issues as well. Journalists, serving in their capacities as members of the press, possess a unique expertise, often from years of experience. Journalistic ethics also impose accountability, demanding that journalists remain credible in the eyes of the public. The significance of journalist credibility is matched only by its fragility, evinced by the public downfall of some of the most prominent members of the press.[144] Judges, on the other hand, have no such expertise, and, at least with respect to federal judges and appointed state judges, remain mostly isolated from the demands of the public. As the Fifth Circuit recognized:

> Courts are not equipped, staffed, or trained to meet the public interest by choosing among the programming interests to be served. Converting courts into super-editors, in derogation of the press freedom guaranteed by

Id. at 518. As surely as the Framers did not anticipate the evolution of sophisticated recording devices, they could not have anticipated the "Cyber Age" we live in today and the technological advances that would produce data security, vulnerabilities, and the discovery thereof.

[139] *Id.* at 535.

[140] *Id*. at 525.

[141] *See supra* Part III(B).

[142] *Bartnicki*, 532 U.S. at 518.

[143] Though not as clearly articulated, the Court in *New York Times Co.* similarly allowed publication regardless of a source's illegal acquisition of information. N.Y. Times Co. v. United States, 403 U.S. 713, 714–15 (1971). When considering the prior restraint, the Court made little of source Daniel Ellsberg's acquisition of the Pentagon Papers, apparently ignoring this aspect and resting its decision on entirely different grounds. *Id*.; *see* O'Neil, *supra* note 135, at 1009. Ultimately, the Justices struck down the prior restraint, despite the fact that the source had stolen the documents. *See N.Y. Times Co.*, 403 U.S. at 713–14. However, writing in dissent, Justice Blackmun exclaimed, "I strongly urge, and sincerely hope, that these two newspapers will be fully aware of their ultimate responsibilities to the United State of America." *Id.* at 762 (Blackmun, J., dissenting).

[144] *See, e.g., More Fallout from Brian Williams Reporting Scandal*, CBS NEWS (Feb. 20, 2015), http://www.cbsnews.com/news/more-fallout-from-brian-williams-reporting-scandal/; *CBS News Admits Bush Documents Can't Be Verified*, NBC NEWS, http://www.nbcnews.com/id/6055248/ns/politics/t/cbs-news-admits-bush-documents-cant-be-verified/#.VOv6iPnF-8A (last updated Sept. 21, 2004).

> the First Amendment, would be not only unprecedented, unwise, and unwelcome; it would be unconstitutional.[145]

¶54 Of course, the press might sometimes make irresponsible decisions when deciding what stories to publish. But this alone does not justify judicial or legislative intervention: "A responsible press is an undoubtedly desirable goal, but press responsibility is not mandated by the Constitution and like many other virtues it cannot be legislated."[146] The First Amendment ensures that news editors maintain discretion to determine what material to publish. Governmental adoption of a responsible disclosure policy would restrict the press's speech on an issue of public concern, which the First Amendment was specifically designed to prevent. Barring extreme circumstances, the government cannot regulate this editorial function without violating one of the most fundamental constitutional guarantees.[147]

V. POLICY CONSIDERATIONS

¶55 Inhibiting the disclosure of data vulnerabilities also raises various policy concerns. Part V(A) discusses how allowing vulnerability disclosures encourages speech about data security, whereas a responsible disclosure policy, like any other prior restraint, creates a chilling effect on the beneficial dissemination of vital information. In light of this likely chilling effect, Part V(B) turns to how disclosure facilitates resolution of data vulnerabilities and mitigates the severity of harm caused by breaches. Part V(C) evaluates this Article's assertions by analyzing the "Heartbleed bug," which initially caused panic in early 2014.

A. Public Debate and Chilling Effects

¶56 At the heart of the First Amendment is our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[148] And as Chief Justice Warren Burger stated, "A prior restraint, by contrast and by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanctions after publication 'chills' speech, prior restraint 'freezes' it at least for the time."[149] As discussed *supra* Part III(B), data security is undoubtedly a matter of public concern, and its growing influence on daily life is unlikely to abate. As technology develops, the collection and storage of important data correspondingly increases, causing data security and privacy to become steadily more vital. This

---

[145] Muir v. Ala. Educ. Television Comm'n, 656 F.2d 1012, 1024 (5th Cir. 1981), *aff'd in part, rev'd in part*, 688 F.2d 1033 (5th Cir. 1982).

[146] Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 256 (1974).

[147] *Id*. at 258 ("The choice of material to go into a newspaper . . . and treatment of public issues and public officials—whether fair or unfair—constitute the exercise of editorial control and judgment. It has yet to be demonstrated how governmental regulation of this crucial process can be exercised consistent with First Amendment guarantees of a free press as they have evolved to this time."); *see also id.* at 261 (White, J., concurring) ("[W]e have never thought that the First Amendment permitted public officials to dictate to the press the contents of its news columns or the slant of its editorials.").

[148] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

[149] Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

unprecedented societal reliance on highly complex innovation warrants robust public debate.

¶57 But adopting a responsible disclosure policy would inhibit public discourse over data security. Indeed, responsible disclosure would not merely chill debate[150] but freeze it at its most critical moments—when data is no longer secure. In an effort to protect business interests, this policy would sacrifice public knowledge for consumer ignorance, making reputational damage-control more manageable for data-holders after a breach. Ultimately, inhibiting disclosure would keep the "marketplace of ideas" from serving its historic function.

¶58 In a similar vein, a responsible disclosure policy would spark public antipathy.[151] In light of the widespread public fear discussed *supra* Part III(B), consumers are unlikely to respond positively after discovering data-holders concealed information of a breach, especially if prompt notification could have mitigated any inflicted harm. On the contrary, disclosure works as an equalizing force, letting consumers gain some semblance of control over their personal information. Speaking of the importance of robust public debate and equal access, security-expert Bruce Schneier suggests:

> This democratization is important. If a known vulnerability exists . . . [w]ord will eventually get out—the [w]indow of [e]xposure will grow—but you have no control, or knowledge, of when or how. All you can do is hope that the bad guys don't find out before the good guys fix the problem. Full disclosure means that everyone gets the information at the same time, and everyone can act on it.[152]

¶59 By giving consumers the opportunity to engage in self-help, equal access to information about data vulnerabilities essentially works as a safety valve, allowing individuals to ensure their financial wellbeing. Few policy choices are more reviled than those that restrict the dissemination of vital information.[153] Any policy that limits disclosure deters critically-important information from reaching the public when it is most necessary, ultimately harming not only those affected by a breach, but also consumer confidence as a whole.

B. Corporate Accountability and Vulnerability Resolution

¶60 Vulnerability disclosures also inspire data security innovation. Unrestrained disclosure places a prospective burden on data-holders, acting as both a catalyst for change and a market constraint. In short, vulnerability disclosures promote fundamental, free-market economic principles. In Professor Eugene Volokh's words:

---

[150] *See generally* Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U. L. REV. 685, 689 (1978) ("The very essence of a chilling effect is an act of deterrence.").

[151] *See* Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1111–21 (2005).

[152] Schneier, *supra* note 20.

[153] *See, e.g.,* Jerry J. Berman, *The Right to Know: Public Access to Electronic Information*, *in* 2 NEW DIRECTIONS IN TELECOMMUNICATIONS POLICY: INFORMATION POLICY AND ECONOMIC POLICY 39, 55 (Paula R. Newberg ed. 1989) ("Congress and a broad public interest and information industry coalition roundly condemned . . . [the Department of Defense's] plans as a threat to the free flow of information. As a consequence, the policy directive . . . was rescinded and legislation was passed to restrict [the Department of Defense's] authority to set computer security policy for unclassified data systems.").

> Publishing detailed information about a computer program's security vulnerabilities may help security experts figure out how to fix the vulnerabilities, persuade apathetic users that there really is a serious problem, persuade the media and the public that some software manufacturer isn't doing its job, and support calls for legislation requiring manufacturers to do better.[154]

Professor Volokh highlights two important facets of vulnerability speech—it encourages both commercial accountability and security breach resolution.

¶61 Vulnerability disclosures facilitate data-holder accountability and boost economic growth through marketplace competition based on perceived security strength.[155] Addressing the accountability issue during a Senate Judiciary Committee hearing following the Target breach, Senator Mike Lee stated, "I generally trust the market to create the right incentives for retailers to protect data of their customers. But consumers need notification of data breaches for that to work."[156] In practice, allowing nondisclosure of data vulnerabilities leads to companies placing less of a priority on rectifying the breach; unsurprisingly, these same companies are less likely to communicate an actual breach to the public.[157] Public disclosure, or even the threat thereof, may serve as the primary motivating factor for speedy vulnerability resolution.[158] For instance, HP's 2015 *Cyber Risk Report* found that nearly half of the attacks that occurred in 2014 exploited two- to four-year-old vulnerabilities, revealing the importance of this public-disclosure motivation.[159] Ultimately, "security through obscurity" is ineffective.[160]

---

[154] Volokh, *supra* note 151, at 1118.

[155] *See generally* Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J. TELECOMM. & HIGH TECH. L. 163 (2004) (suggesting a multifactor-based disclosure model to balance security and privacy interests).

[156] *Summary: Target Testifies on Massive Data Breach*, *supra* note 14.

[157] *See* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 181–82 (2005); *see also supra* notes 10–11 and accompanying text (describing Skype's failure to resolve or report a significant vulnerability in a timely fashion). For additional examples of companies forgoing or delaying notification, see Kevin Burke, *Virgin Mobile Fails Web Security 101, Leaves Six Million Subscriber Accounts Wide Open*, KEVIN BURKE (Sept. 17, 2012), http://kev.inburke.com/kevin/open-season-on-virgin-mobile-customer-data/ (accounting for Virgin Mobile's failure to address or disclose a vulnerability after extensive notification by the researcher who discovered it); *Exploit Sat on LA Times Website for 6 Weeks*, KREBS ON SECURITY (Feb. 13, 2013), http://krebsonsecurity.com/2013/02/exploit-sat-on-la-times-website-for-6-weeks/ (describing the *Los Angeles Times*'s failure to identify a vulnerability for six weeks despite notification by readers and an outside security expert identifying it as malware); Eduard Kovacs, *Experts Find Code Execution Flaw in PS3, Password Reset Bug in Sony Entertainment Network*, SOFTPEDIA (May 29, 2013, 12:41 PM), http://news.softpedia.com/news/Experts-Find-Code-Execution-Flaw-in-PS3-Password-Reset-Bug-in-Sony-Entertainment-Network-356623.shtml (describing Sony's failure to address a high-severity security flaw for five months, at which point the researchers publicly disclosed information about the vulnerability); *see also Vulnerability Disclosure Policy*, CERT/CC, http://www.cert.org/kb/vul_disclosure.html (last visited Mar. 1, 2015) (providing that the company has the discretion to choose to never disclose some vulnerabilities).

[158] *See* Bruce Schneier, *Internet Shield: Secrecy and Security*, S.F. CHRON. (Mar. 2, 2003), *available at* http://www.schneier.com/essay-033.html.

[159] HP SECURITY RESEARCH, CYBER RISK REPORT (Feb. 2015), *available at* https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-0858enw.pdf.

[160] *See, e.g.,* Matwyshyn, *supra* note 157; Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1337 (2006). That said, this Author recognizes that "[t]he proliferation of publications providing

¶62 Nevertheless, some companies support disclosure, recognizing its utility in promoting expeditious resolution of high-risk data vulnerabilities. Most notably, in 2013 Google adopted a revised policy for when its security researchers discover exploitation of publicly unknown "zero-day" vulnerabilities.[161] Under this policy, Google would notify vendors upon discovery of data vulnerabilities that they had sixty days to resolve critical vulnerabilities and only seven days to resolve vulnerabilities being actively exploited.[162] If left unresolved, Google would take steps to "support researchers making details available so that users can take steps to protect themselves."[163] Many companies, such as TippingPoint and Facebook, have similar programs encouraging outside researchers and individual users to notify them of data security vulnerabilities.[164] These initiatives often recognize the importance of both giving customers the opportunity to engage in self-help and allowing companies to rectify data vulnerabilities internally. For instance, TippingPoint's "Zero Day Initiative" details:

> In order to maintain the secrecy of a researcher's vulnerability discovery until a product vendor can develop a patch, TippingPoint customers are only given a generic description . . . . In other words, TippingPoint customers will be protected from the vulnerability in advance, but they will not be able to discern the vulnerability itself.[165]

These programs and policies not only promote resolution of vulnerabilities, but also alert the public to take protective measures, such as by avoiding certain programs or websites, monitoring personal accounts, and changing passwords.[166]

¶63 Vulnerability disclosures also indirectly facilitate consumer self-help by promoting cybersecurity expertise. Despite an increasing need, few individuals qualify as cybersecurity experts, forcing the public to rely on the advice of a small community of IT

---

information about vulnerabilities and programs that exploit vulnerabilities has enlarged the population of computer users capable of successfully breaching computer security." Preston & Lofton, *supra* note 88, at 78. However, this goes hand-in-hand with the increased population of users capable of successfully improving computer security and resolving the issues.

[161] *See* Evans & Hintz, *supra* note 23.

[162] *See id*. When Google established Project Zero in 2014, it revised this policy to a 90-day deadline. *See* Chris Evans, *Announcing Project Zero*, GOOGLE PROJECT ZERO BLOG (July 15, 2014, 5:30 AM), http://googleprojectzero.blogspot.com/2014/07/announcing-project-zero.html.

[163] *See id*. Many companies have adopted similar, though not as stringent, policies to compel resolution of data vulnerabilities. *See, e.g., Disclosure Policy*, SECUNIA, http://secunia.com/community/research/policy/ (last visited Aug. 3, 2014); *ICS-CERT Vulnerability Disclosure Policy*, ICS-CERT, http://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy (last visited Aug. 3, 2014); *Vulnerability Disclosure Program*, SOLUTIONARY, http://www.solutionary.com/research/vulnerability-disclosure-program/ (last visited Aug. 3, 2014).

[164] *See Information*, FACEBOOK, https://www.facebook.com/whitehat (last visited Aug. 3, 2014) (defining a policy offering bounties for responsibly reporting bugs); *Increased Rewards for Google's Web Vulnerability Reward Program*, GOOGLE ONLINE SECURITY BLOG, http://googleonlinesecurity.blogspot.com/2013/06/increased-rewards-for-googles-web.html (last visited Aug. 3, 2014) (outlining a program to reward researchers who submit vulnerability reports regarding Google's services); *Zero Day Initiative*, TIPPINGPOINT, http://www.zerodayinitiative.com/about/ (last visited Aug. 3, 2014) (detailing an initiative to pay researchers to report security bugs to independent firms).

[165] *Zero Day Initiative*, TIPPINGPOINT, *supra* note 164.

[166] "Computer owners and operators who are aware of a potential vulnerability can take steps to fix it, while they are powerless to fix an unknown vulnerability." Preston & Lofton, *supra* note 88, at 81.

professionals.[167] These experts thus stand at the vanguard of data security accountability, helping the public determine who to trust in the cyber marketplace. Without this guidance, consumers would be unable to make informed decisions when divulging personal information to potential data-holders. In turn, companies without proper data security measures in place would remain unconstrained by market forces. Worse yet, determining the extent of one's online exposure is difficult, causing many consumers to traverse the Internet without knowing where and with whom their personal data is stored.[168] The opacity of data-holders' identities would further increase without accountability, magnifying the current risk of harm from a breach. Given these points, cybersecurity experts decrease both individual and systemic risk by empowering the public to act as prudent decision-makers.

¶64 Vulnerability disclosures provide crucial information for security experts to solve these issues before they arise. Jennifer Granick, Director of Civil Liberties at the Stanford Center for Internet and Society, emphasizes that restrictions on vulnerability publications would discourage the development of computer-security technologies because innovation requires open access, peer review, and experimental replication.[169] Publications of data vulnerabilities permit the data security community to collaborate and collectively address misrepresentations or weaknesses, acting as "'fact-checkers' of the information technology ecosystem."[170] This ultimately strengthens security systems and increases the availability of the most advanced security technologies.[171] Thus, concealing data weakness discoveries potentially inflicts harm not only upon those affected by a specific

---

[167] *See* Eric Beidel & Stew Magnuson, *Government, Military Face Severe Shortage of Cybersecurity Experts*, NAT'L DEFENSE MAG. (Aug. 2011), http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx (describing the high demand for cybersecurity experts in government work); Carric Dooley, *Recruit, Reward & Retain Cybersecurity Experts*, MCAFEE (Jan. 20, 2015), https://blogs.mcafee.com/executive-perspectives/recruit-reward-retain-cybersecurity-experts (describing the cybersecurity expert shortage and how to recruit these experts); *see also* Ali Qamar, *How to Become a Cyber Security Expert*, INFOSEC INST. (Dec. 24, 2014), http://resources.infosecinstitute.com/become-cyber-security-expert/ (providing advice for becoming an expert in cybersecurity, recognizing that "strenuous work is expected").

[168] *See* Preston & Lofton, *supra* note 88, at 138–39.

[169] *See* Jennifer Stisa Granick, *The Price of Restricting Vulnerability Publications*, 9 INT'L J. COMM. L. & POL'Y 1 (2005). Famed commentator Eugene Volokh further notes:

> Discussions of computer security problems, or of encryption or decryption algorithms, can educate computer programmers who are working in the field or who are studying the subjects . . . create new algorithms and security systems. Scientific research is generally thought to advance more quickly when scientists and engineers are free to broadly discuss their work.

Volokh, *supra* note 151, at 1112.

[170] Matwyshyn, *Hacking Speech*, *supra* note 23, at 821. Matwyshyn also highlights that "our future as a viable country may literally depend on the security improvements vulnerability speech may trigger." *Id*. at 817.

[171] *See id*. at 817–22 ("When information security researchers expose flaws in code, their vulnerability speech highlights ways that systems can be attacked by malefactors. But in doing so they trigger critical debate around information security, and ideally, the vulnerable systems become strengthened as a result of the speech."); Preston & Lofton, *supra* note 88, at 81 ("Computer security publications provide long-term benefits as vulnerabilities are corrected and better products reach the market. Computer owners and operators who are aware of a potential vulnerability can take steps to fix it, while they are powerless to fix an unknown vulnerability.").

security breach, but also upon all those who suffer from otherwise preventable breaches had security experts been given the opportunity to learn from the prior breach. Any legislative or judicial action inhibiting disclosure would consequently stunt the development of innovative protective technologies. In the end, the paternalism inherent to a responsible disclosure policy restricts freedom of choice, limits competition, thwarts innovation, and inhibits public discourse.

C. Heartbleed Bug: A Case Study

¶65 The recent discovery of a major vulnerability in OpenSSL highlights the importance of vulnerability speech.[172] In early 2014, a Google researcher and Codenomicon, a security firm, discovered what became known as the "Heartbleed bug."[173] Codenomicon issued a release describing the threat:

> The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.[174]

Although parties originally planned to disclose the bug in a week's time, security researchers decided to alert the public after recognizing the magnitude of the threat.[175] In the aftermath, and despite it affecting two-thirds of all Internet websites, public disclosure provided clear benefits, expediting vulnerability resolution, increasing data-holder accountability, and mitigating public harm.

¶66 After disclosure, websites raced to resolve any data vulnerabilities. While many succeeded admirably, for those that struggled to rectify the threat, reputational damages ensued.[176] The availability of test-sites and browser extensions, which expose unsecure websites, placed additional pressure on data-holders to repair any weaknesses quickly and

---

[172] OpenSSL is an open-source implementation of Secure Socket Layer (SSL), a cryptographic protocol that ensures that data passed between a web server and a browser is secure and private. For a more detailed, yet accessible, explanation of OpenSSL, see Jakub Kasztalski, *OpenSSL: What Is It and Why Is It Needed*, GUARDIAN LIBERTY VOICE (June 8, 2014), http://guardianlv.com/2014/06/openssl-what-is-it-and-why-is-it-needed/.

[173] Lily Hay Newman, *Popular Encryption Software's "Heartbleed" Bug Leaks Information*, SLATE (Apr. 8, 2014, 4:09 PM), http://www.slate.com/blogs/future_tense/2014/04/08/heartbleed_openssl_encryption_bug_discovered_by_codenomicon_and_neel_mehta.html. Google and Codenomicon discovered the Heartbleed bug independently of one another, but at roughly the same time. *Id.*

[174] *The Heartbleed Bug*, CODENOMICON, http://heartbleed.com/ (last accessed Feb. 24, 2015).

[175] For a complete timeline of the discovery and disclosure of the Heartbleed Bug, see Ben Grubb, *Heartbleed Disclosure Timeline: Who Knew What and When*, SYDNEY MORNING HERALD (Apr. 15, 2014), http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html.

[176] *See* Rachael King & Steven Norton, *Google, Microsoft Race to Assess Heartbleed Vulnerability*, WALL ST. J. (Apr. 8, 2014, 6:31 PM), http://blogs.wsj.com/cio/2014/04/08/google-microsoft-race-to-assess-heartbleed-vulnerability/. It should be noted that some companies were given advance notice and the opportunity to patch their sites before the news was disclosed. *See* Grubb, *supra* note 175.

completely.[177] In effect, these test-sites allowed consumers to determine which websites to avoid, thus reducing consumer traffic for websites unable to ensure data security.[178]

¶67 But perhaps most striking was the media's role. While the vast majority of vulnerable websites refrained from notifying users of potential harm,[179] the media made up for this failure, providing information—often in easy-to-understand charts and diagrams—about vulnerable sites and which passwords to change.[180] According to one study by the Pew Research Center, this press coverage reached 64% of Internet users, prompting approximately two-thirds of these users—or 39% of all Internet users—to take protective measures, such as by changing their passwords.[181] Timely disclosure thus enabled the public to engage in self-help, avoiding a data security calamity of unimaginable proportions. What damage would have occurred without prompt public disclosure is unknown. What we do know, however, is that if the media had not played such an integral role in notifying the public, many of these mitigating efforts would not have occurred.

VI. OTHER LEGAL CONSIDERATIONS

¶68 The vulnerability-speech debate does not occur in a legal vacuum. Other than First Amendment jurisprudence, commentators identify various fields of law beyond the intended scope of this Article, such as intellectual property law and privacy law, which may affect vulnerability-speech interests in certain situations.[182] Contract and agency law, however, are pertinent to this Article's analysis.

¶69 The unique relationship between cybersecurity experts and data-holders potentially limits First Amendment rights. Conscientious data-holders engage cybersecurity experts to mitigate the threat of a data breach. Because this likely requires access to proprietary information, contracts detailing these arrangements are understandably replete with nondisclosure obligations. Coupled with the ability to access highly sensitive

---

[177] *See, e.g., Chromebleed*, CHROME WEB STORE, https://chrome.google.com/webstore/detail/chromebleed/eeoekjnjgppnaegdjbcafdggilajhpic (last visited Aug. 29, 2014); *LastPass Heartbleed Checker*, LASTPASS, https://lastpass.com/heartbleed/ (last visited Aug. 29, 2014).

[178] *See* Brian Krebs, *Heartbleed Bug: What Can You Do?*, KREBS ON SECURITY (Apr. 14, 2014), http://krebsonsecurity.com/2014/04/heartbleed-bug-what-can-you-do/.

[179] Some notable exceptions include Amazon Web Services, LastPass, Pinterest, Prezi, SoundCloud, Tumblr, Turbotax, and Wikipedia, all of which publicly announced the data vulnerabilities resulting from the Heartbleed Bug.

[180] *See, e.g.,* Jason Cipriani, *Heartbleed Bug: Check Which Sites Have Been Patched*, CNET (Apr. 9, 2014, 2:54 PM), http://www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug/; *The Heartbleed Hit List: The Passwords You Need to Change Right Now*, MASHABLE (Apr. 9, 2014, 11:00 AM), http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/; Molly Wood, *Flaw Calls for Altering Passwords, Experts Say*, N.Y. TIMES (Apr. 9, 2014), http://www.nytimes.com/2014/04/10/technology/flaw-calls-for-altering-passwords-experts-say.html.

[181] Lee Rainie & Maeve Duggan, *Heartbleed's Impact*, PEW RESEARCH INTERNET PROJECT (Apr. 30, 2014), *available at* http://www.pewinternet.org/2014/04/30/heartbleeds-impact/.

[182] This Article will not address these ancillary legal implications, but it is important to note that various legal principles might be relevant to further analysis. For additional reading, consider: Susan W. Brenner, *Complicit Publication: When Should the Dissemination of Ideas and Data Be Criminalized?*, 13 ALB. L.J. SCI. & TECH. 273 (2003); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1998); Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777 (2007).

information, a cybersecurity expert's specialized know-how creates the potential for abuse. Whether through faulty advice or the exploitation of confidential information, a security researcher can cause widespread harm, affecting both the data-holder and all those who trusted the data-holder with protecting their personal information. As a result, special duties may extend beyond those defined via contract. Determining the existence and scope of special duties stemming from a trust-based relationship requires fact-specific analysis.

¶70 Government employees with knowledge of sensitive information, for instance, might incur heightened obligations limiting free speech. In *Snepp v. United States*, the CIA sued a former agent after he published a book about the CIA's involvement in South Vietnam based on his experience as an agent.[183] Snepp had signed a contract agreeing "not [to] publish . . . any information or material relating to the Agency, its activities or intelligence activities generally, either during or after the term of [his] employment . . . without specific prior approval by the Agency."[184] Essentially, the contract required prior clearance to disclose any information related to the CIA—whether fact or opinion, and regardless of its confidentiality.[185] Thus, even though the parties stipulated that Snepp had not disclosed any classified information, Snepp had nevertheless breached his employment contract when he chose not to submit his book for prior approval.[186] The more nebulous question was if this breach warranted imposing a constructive trust.[187]

¶71 The Court held that the contract was valid, including its prepublication review process, and that a constructive trust was proper, requiring Snepp to assign all profits resulting from the sale of the book to the CIA.[188] The Court recognized:

> Snepp's employment with the CIA involved an extremely high degree of trust. In the opening sentence of the agreement that he signed, Snepp explicitly recognized that he was entering a trust relationship. The trust agreement specifically imposed the obligation not to publish any information relating to the Agency without submitting the information for clearance. . . . He deliberately and surreptitiously violated his obligation to submit all material for prepublication review. Thus, he exposed the classified information with which he had been entrusted to the risk of disclosure.[189]

The Court emphasized Snepp's fiduciary duties and contractual obligations to the CIA.[190] But as Justice Stevens noted in dissent, a constructive trust is typically a remedy for unjust enrichment resulting from the breach of a fiduciary duty.[191] If Snepp had disclosed and profited from classified information, then he would have violated his duty of loyalty

[183] 444 U.S. 507 (1980).
[184] *Id.* at 513.
[185] *Id*. at 508.
[186] *Id.* at 513.
[187] *Id.* at 511.
[188] *Id*. at 510–12, 515.
[189] *Id*. at 510–11.
[190] *Id.* at 510–12, 515.
[191] *Id.* at 519 (Stevens, J., dissenting).

to the CIA, which would have warranted imposing a constructive trust.[192] However, Snepp had not disclosed classified information, instead breaching the terms of his employment contract requiring prepublication approval.[193] Unlike a simple breach of contract, which would have resulted in, at worst, punitive damages, the Court interpreted Snepp's obligation to submit publications for prior approval as a fiduciary duty.[194] In sum, Snepp's obligations extended beyond those defined in his employment contract because a trust-based relationship imposed special duties.

¶72 Even outside the government-employment context, security researchers may find themselves similarly bound by both an employment contract and a fiduciary-like relationship. Analogous to the relationship between the CIA and its former agent, a security researcher employed by or under contract with a data-holder might face comparable legal backlash upon public disclosure of a data vulnerability. Contractually, this arrangement could take the form of a responsible-disclosure notification policy or a nondisclosure agreement, either restricting the individual's right to disclose news about the vulnerability—with prepublication notice or other means functioning like prepublication review—or imposing contractual remedies following publication of a breach.[195]

¶73 Moreover, contractual duties may prevent parties who are otherwise unaffiliated with the data-holder from publishing news of a data vulnerability. For instance, creating an account on a data-holder's website—a potentially necessary step in the discovery of a vulnerability—may impose certain duties restricting vulnerability speech, such as those found in a Terms of Service agreement.[196] Additionally, in the software context, an end-user license agreement (EULA) may include a "no reverse engineering" clause or similar limitations that affect the user's right to release data about the software's performance.[197] These agreements can impose different degrees of protection for data-holders, ranging

---

[192] *Id.*

[193] *Id.*

[194] *See id.*

[195] For example, NDAs frequently appear in the testing industry. When e-voting systems were rising to prominence, the computer consultants who contracted to test the security of the voting software were expected to sign NDAs. This troubled voting activists, who were then unable to obtain information to judge the impartiality, fairness, or completeness of the testing process. Kim Zetter, *E-Voting Tests Get Failing Grade*, WIRED (Nov. 1, 2004), http://archive.wired.com/politics/security/news/2004/11/65535?currentPage=all. NDAs may also be relevant outside of the employment context. For example, if Android discovers or is notified of a dangerous security vulnerability, its security team's first step is to notify companies who have signed NDAs—those who are restricted from publishing information about the vulnerability until there has been a fix. Android will not publish until a patch has been provided to these companies. It requires NDAs "to ensure that the security issue does not become public prior to availability of a fix and put users at risk." *Security Updates and Resources*, ANDROID, https://source.android.com/devices/tech/security/overview/updates-resources.html (last visited Mar. 3, 2015).

[196] *See Coders' Rights Project Vulnerability Reporting FAQ*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/coders/vulnerability-reporting-faq (last visited Mar. 3, 2015) ("Websites or other internet services also may [have] TOS or TOU that purport to restrict otherwise legal research activities."). This becomes particularly troublesome when a researcher can only gain access to the site to discover a vulnerability by setting up an account.

[197] *See id.*; *see, e.g.,* ADOBE, ADOBE ACCESS END USER LICENSE AGREEMENT, *available at* http://www.adobe.com/content/dam/Adobe/en/products/adobe-access/pdfs/adobe-access-trial-eula-en-06252012-2108.pdf (last visited Mar. 3, 2015); *Alt-N Software End User License Agreement*, ALT-N, http://www.altn.com/Company/Policies/Software-EULA/#Confidentiality (last visited Mar. 3, 2015) (including a "Confidentiality and No Reverse Engineering" clause).

from blanket prohibitions forbidding disclosure to specific parameters detailing the content of a disclosure should a discovery occur.

¶74 Beyond contractual obligations, the nature of the relationship between a data-holder and security researcher can cause principal–agent duties to arise. In *Snepp*, although the Court looked to the employment contract to justify finding in favor of the CIA, fiduciary duties can nevertheless arise in the absence of a contract should a similar trust-based relationship exist between parties.[198] While the question of whether security researchers are subject to these heightened duties likely requires fact-specific, case-by-case analysis, both the highly technical level of expertise required and the sensitivity of the information involved increase the likelihood of a court finding the existence of a fiduciary relationship.[199] If a principal–agent relationship exists, the corresponding duties of care and loyalty might preclude security researchers from publically disclosing data vulnerabilities, even in egregious circumstances, because disclosure would not be in the best interests of the company.

VII. CONCLUSION

> Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period.[200]

¶75 With the rapid development and expansion of technology and the Internet, data security is one of today's exigencies, the importance of which is unlikely to wane. Data security breaches are not an anomaly, neither in their frequency nor in scope.[201] For instance, in the fall of 2014, a data breach involving Home Depot surpassed the magnitude of the Target breach, with fifty-six-million credit-card numbers stolen over a period of five months.[202] Target and Home Depot are not alone. In just one month, among

---

[198] *See, e.g.,* Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984) (upholding a protective order that prevented a defendant newspaper from disclosing the plaintiff organization's membership and donor lists as they received the information during a defamation trial's discovery phase and thus were bound not to misuse the information). This duty may be created by the nature of the position. *See, e.g.,* United States v. Aguilar, 515 U.S. 593, 606 (1995) ("Government officials in sensitive confidential positions may have special duties of nondisclosure.").

[199] *See* Jones v. United States, 703 F.2d 246, 251 (7th Cir. 1983) (extending liability when a defendant accepted "a discrete task, . . . [involving] special knowledge or expertise"); *see also* RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 43 (Tentative Draft 2005) (equating a breach of fiduciary duty with a breach of a "duty imposed by a relation of trust or confidence"); *see id.* cmt. f ("[T]he confidential character of a relationship normally described as 'fiduciary' . . . will be presumed, while the confidential character of a relation outside the standard fiduciary models must be proved as a matter of fact in a particular case.").

[200] Thornhill v. Alabama, 310 U.S. 88, 102 (1940).

[201] For a complete record of the 4,489 data breaches made public since 2005, see *Chronology of Data Breaches Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last visited Mar. 3, 2015).

[202] Brian Krebs, *Banks: Credit Card Breach at Home Depot*, KREBS ON SECURITY (last updated Sept. 2, 2014, 1:50 PM), http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/; Paula Rosenblum, *Home Depot Data Breach: Banks' Response Is Critical to Consumer Reaction*, FORBES (Sept. 19, 2014, 10:30 AM), http://www.forbes.com/sites/paularosenblum/2014/09/19/home-depot-data-breach-

others, J.P. Morgan, Apple, Kmart, Dairy Queen, MBIA, and Snapchat suffered significant data breaches.[203] Moreover, data security breaches increasingly catch the public's attention, evidenced in the recent attack on Sony, which prevented, albeit partially, the cinematic release of *The Interview*.[204]

¶76 In the end, collaboration and communication are essential to resolving these issues. As Target's Chief Financial Officer recognized, "[O]ne of the keys going forward is sharing information across the industry, so we can all understand revolving threats and respond to them."[205] A robust debate focusing on data security needs to take place among the public and experts alike.[206] Relevant information needs to be open and accessible to achieve this goal.

¶77 Through either legislation or judicial mandate, a responsible disclosure policy would amount to a prior restraint, which the narrow national-security exception fails to justify. Importantly, rejecting a responsible disclosure policy as a prior restraint would not preclude criminalizing unauthorized access or otherwise regulating the dissemination and exploitation of personal or financial information. Further, the absence of a responsible disclosure policy does not affect post-publication liability (e.g., defamation, publication of private facts, copyright infringement, etc.) under federal or state law. As discussed in this Article, the vulnerability disclosure debate must take into account not only constitutionally protected rights under the First Amendment, but also the practical consequences of chilling the dissemination of vitally beneficial information. In an effort to avoid both limiting the development of enhanced data security safeguards and restricting the public's ability to engage in self-help, Congress and the judiciary should allow basic market forces to pave the way for innovation in this continually evolving field.

---

banks-response-is-critical-to-consumer-reaction/.

[203] *Kmart Investigating Payment System Breach*, KMART (Oct. 10, 2014), http://www.kmart.com/en_us/dap/statement1010140.html?adcell=hpnewsrelease; Sean Gallagher, *Update: FBI, Apple Investigating Celebrity Photo Hacks*, ARS TECHNICA (Sept. 2, 2014, 11:25 AM), http://arstechnica.com/tech-policy/2014/09/fbi-apple-investigating-celebrity-photo-hacks/; Brian Krebs, *Huge Data Leak at Largest U.S. Bond Insurer*, KREBS ON SECURITY (Oct. 7, 2014), http://krebsonsecurity.com/2014/10/huge-data-leak-at-largest-u-s-bond-insurer/; Maggie McGrath, *JP Morgan Says 76 Million Households Affected by Data Breach*, FORBES (Oct. 2, 2014, 5:51 PM), http://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/; Paula Mejia, *"The Snappening" Hack May Leak up to 200,000 Sensitive Snapchat Photos*, NEWSWEEK (Oct. 11, 2014, 1:48 PM), http://www.newsweek.com/snappening-hack-may-leak-200000-sensitive-snapchat-photos-276896; Kate Vinton, *Data Breach Bulletin: Dairy Queen, JP Morgan Chase, AT&T*, FORBES (Oct. 10, 2014, 12:42 PM), http://www.forbes.com/sites/katevinton/2014/10/10/data-breach-bulletin-dairy-queen-jp-morgan-chase-att/.

[204] Christopher Palmeri, Anousha Sakoui & Lucas Shaw, *Sony Hackers Expose Rogen's Pay Along with Deloitte Salaries*, BLOOMBERG (Dec. 4, 2014, 2:12 PM), http:/www.bloomberg.com/news/2014-12-03/sony-hackers-expose-rogen-s-pay-along-with-salaries-at-deloitte.html.

[205] *Summary: Target Testifies on Massive Data Breach*, *supra* note 14.

[206] For example, Google's recent exposure of a Windows vulnerability has productively reignited the disclosure policy debate amongst data-holders and security researchers. *See Issue 18*, GOOGLE SECURITY RESEARCH, https://code.google.com/p/google-security-research/issues/detail?id=118 (last visited Mar. 4, 2015); *see also* Sean Gallagher, *Google Updates Disclosure Policy After Windows, OS X Zero-Day Controversy*, ARS TECHNICA (Feb. 13, 2015, 3:32 PM), http://arstechnica.com/security/2015/02/google-updates-disclosure-policy-after-windows-os-x-zero-day-controversy/; Chris Strohm & Jordan Robertson, *Google Threatens to Air Microsoft and Apple's Dirty Code*, BLOOMBERG (Feb. 11, 2015, 5:00 AM), http://ww.bloomberg.com/news/articles/2015-02-11/google-riles-silicon-valley-by-exposing-others-security-flaws.