Pace Intellectual Property, Sports & Entertainment Law Forum

Volume 7
Issue 1 *Spring 2017*

Article 1

June 2017

# Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the Modern World

Conrad Wilton
*Fox Rothschild LLP*

# Sony, Cyber Security, and Free Speech: Preserving the First Amendment in the Modern World


## Abstract

Reprinted from 16 U.C. Davis Bus. L.J. 309 (2016). This paper explores the Sony hack in 2014 allegedly launched by the North Korean government in retaliation over Sony's production of The Interview and considers the hack's chilling impact on speech in technology. One of the most devastating cyber attacks in history, the hack exposed approximately thirty- eight million files of sensitive data, including over 170,000 employee emails, thousands of employee social security numbers and unreleased footage of upcoming movies. The hack caused Sony to censor the film and prompted members of the entertainment industry at large to tailor their communication and conform storylines to societal standards. Such censorship cuts the First Amendment at its core and exemplifies the danger cyber terror poses to freedom of speech by compromising Americans' privacy in digital mediums. This paper critiques the current methods for combatting cyber terror, which consist of unwieldy federal criminal laws and controversial information sharing policies, while proposing more promising solutions that unleash the competitive power of the free market with limited government regulation. It also recommends legal, affordable and user-friendly tools anyone can use to secure their technology, recapture their privacy and exercise their freedom of speech online without fear of surreptitious surveillance or retaliatory exposure.



## Keywords

cybersecurity, cyber security, first amendment, terrorism, cyber terrorism


## Cover Page Footnote

Reprinted from 16 U.C. Davis Bus. L.J. 309 (2016).

PACE INTELLECTUAL PROPERTY, SPORTS & ENTERTAINMENT LAW FORUM

VOLUME 7 SPRING 2017 NUMBER 1

# SONY, CYBER SECURITY, AND FREE SPEECH: PRESERVING THE FIRST AMENDMENT IN THE MODERN WORLD

CONRAD WILTON*

## TABLE OF CONTENTS



* Conrad Wilton is best known as the host of "Conrad's Corner®" Radio - Est. 2010. He graduated from the UC Davis School of Law in 2016 after earning his Bachelor of Arts in broadcast journalism at the University of Southern California in 2013. Conrad currently works in entertainment litigation and transactional law as an associate attorney with Fox Rothschild LLP in Los Angeles, California. He attributes his continued success to the unconditional love and support of Edward and Beatrice Weiss, Ron and Betty Wilton, Baron Wilton and his incredible dog Hunter.

## I. INTRODUCTION

In November of 2014, Sony Pictures Entertainment fell victim to one of the largest and most devastating cyber attacks in history because of its production of the controversial comedy *The Interview*.[1] The film's plot featured the Central Intelligence Agency (CIA) sending talk show host Dave Skylark (James Franco) and his producer Aaron Rapoport (Seth Rogen) on a mission to interview and assassinate North Korean dictator Kim Jong-un.[2] It yielded mixed reviews and received no Oscar nominations, but *The Interview's* significance far transcends its pure entertainment value.[3] *The Interview* symbolizes Sony's attempt to exercise the most cherished right in the United States of America (U.S.) and a right indispensable to any form of self-governance – the right to free speech and expression.

Incensed by the film's plot, the North Korean government employed approximately 6,000 hackers to wage technological warfare against Sony by decimating its servers and exposing approximately thirty-eight million files of confidential data.[4] The social security numbers and birthdays of over 47,000 Sony employees were obtained, including those of household names like

---

[1] Amelia Smith, *Sony Cyber Attack One of the Worst in Corporate History*, NEWSWEEK (Dec. 12, 2014, 1:14 PM), http://europe.newsweek.com/sony-cyber-attack-worst-corporate-history-thousands-files-are-leaked-289230?rx=us.

[2] *Synopsis for The Interview*, IMDB (2014), http://www.imdb.com/title/tt2788710/ synopsis?ref_=ttpl_pl_syn.

[3] *Oscar Nominations 2015: Full List*, VARIETY (Jan. 15, 2015, 05:38 AM), http://variety.com/2015/film/news/oscar-nominations-2015-full-list-academy-award-nominees-1201405517.

[4] Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 28, 2015, 9:43 AM), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

Conan O'Brien and Sylvester Stallone.[5] The hackers leaked employee medical information, salary spreadsheets, and full copies of upcoming films.[6] The hackers also exposed thousands of executive emails containing embarrassing and offensive messages in reference to entertainment and political giants Angelina Jolie, Jeffrey Katzenberg, Kevin Hart and President Barack Obama.[7]

Most disturbingly, the attack caused Sony to censor several scenes in *The Interview* and suspend its theatrical premiere scheduled for Christmas Day of 2014.[8] Although Sony ultimately released the movie and showed the film in mostly independent theaters nationwide, the hack's chilling impact on free communication and expression infected Hollywood and the entertainment community by encouraging executives, actors, writers and the like to consciously censor the contents of electronic communication in fear of a potential hack and public exposure.[9]

Amidst the wake of the attack, American journalist Frank Bruni penned a powerful editorial in *The New York Times* titled "Hacking Our Humanity" that declared the Sony hack confirms the abolition of privacy in a

---

[5] Jose Pagliery, *The Sony Mega-Hack: What You Need to Know*, CNN MONEY (Dec. 12, 2014, 11:13 AM), http://money.cnn.com/2014/12/09/technology/security/sony-hacking-roundup.

[6] Seth Rosenblatt, *13 Revelations from the Sony Hack*, CNET (Dec. 13, 2014, 9:49 AM), http://www.cnet.com/news/13-revelations-from-the-sony-hack.

[7] William Boot, *Shocking New Reveals from Sony Hack*, THE DAILY BEAST (Dec. 12, 2014, 6:30 AM), http://www.thedailybeast.com/articles/2014/12/12/shocking-new-reveals-from-sony-hack-j-law-pitt-clooney-and-comparing-fincher-to-hitler.html.

[8] William Boot, *Sony Emails Show How the Studio Plans to Censor Kim Jong-Un Assassination Comedy* 'The Interview', THE DAILY BEAST (Dec. 15, 2014, 3:26 AM), http://www.thedailybeast .com/articles/2014/12/15/exclusive-kim-jong-un-assassination-comedy-the-interview-will-allegedly-be-censored-abroad.html.

[9] Noam Cohen, *Surveillance Leaves Writers Wary*, N.Y. TIMES (Nov. 11, 2013), http://www.nytimes.com/2013/11/12/books/pen-american-center-survey-finds-caution-among-members.html.

technologically saturated society.[10] Bruni argued that moments in life where one can be messy, stupid and careless are quickly disappearing as technology renders everyone "naked" and exposed to public scrutiny.[11] Bruni also cited a Pew Research Center study that discovered that an overwhelming majority of Americans seriously question the confidentiality and security of social media, online chats and texts, but very few reduce their dependence on electronic communication.[12] Bruni's solution is to utilize encryption, which can be very effective at protecting data and repelling a hack.[13] However, given the increasing intelligence of hackers, encryption is not bulletproof and should be considered one weapon of many that can be used to thwart an attack.

President Obama and his administration believe increased prosecution and sanctions under the controversial Computer Fraud and Abuse Act (CFAA) will reduce computer crime and restore a semblance of privacy in the digital world.[14] George Washington University Law School Professor Orin Kerr published several influential articles on the CFAA, arguing the statute has grown so broad it punishes ubiquitous and relatively innocent conduct with jail

---

[10] Frank Bruni, *Hacking Our Humanity*, N.Y. Times (Dec. 20, 2014), http://www.nytimes.com/ 2014/12/21/opinion/sunday/frank-bruni-sony-security-and-the-end-of-privacy.html.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Orin S. Kerr, *Obama's Proposed Changes to Computer Hacking Statute: A Deep Dive*, WASH. POST (Jan. 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/ obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive.

time.[15] For example, a user faces one year in prison and/or fine for intentionally accessing a computer for an unauthorized purpose (such as using an employee laptop to check personal email) and thereby obtaining information from that computer.[16] The penalty ratchets to five years if the hack implicates information valued at $5,000 or more.[17] President Obama seeks to increase these penalties, but critics contend a strengthened CFAA will not effectively deter hackers given the difficulty in positively identifying the culprits behind cyber attacks.[18] For example, many still doubt North Korea was the source of the Sony hack despite claims to the contrary by the Federal Bureau of Investigation (FBI).[19] Even if the hackers are positively identified as North Korean government employees, the notion that the U.S. will indict Kim Jong-un or anyone under his thumb is inconceivable since the U.S. lacks an extradition agreement with North Korea.[20]

As opposed to the overzealous prosecution of hackers, a more promising solution is to ally the government with the private sector to combat cyber attacks proactively. California Governor Jerry Brown signed Executive Order B-34-15 in August of 2015 establishing the California Cybersecurity

---

[15] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1581 (2010).
[16] *Id.*
[17] *Id.*
[18] Orin S. Kerr, *Obama's Proposed Changes to Computer Hacking Statute: A Deep Dive*, WASH. POST (Jan. 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/ obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive.
[19] Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 28, 2015), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.
[20] 18 U.S.C. § 3181.

Integration Center to foster information sharing between the private sector and the California government, assess risks to both public and private networks, devise new methods to strengthen cyber security, and improve how cyber threats are identified, understood and managed.[21]

On the federal level, the Cybersecurity Information Sharing Act (CISA) is designed to accomplish similar goals and was signed into law December of 2015 as part of the $1.1 trillion omnibus budget bill.[22] Supporters claim CISA is a promising alternative to the current practice of several organizations working independently to combat cyber terror, which puts both public and private entities at considerable risk.[23] However, critics believe the Act will set a dangerous precedent of transferring individuals' personal information to intelligence and law enforcement entities, effectively enabling the government to more easily surveil its citizens notwithstanding Fourth Amendment protections.[24]

This paper argues that cyber security is a public right that requires both government regulation and free market competition to be adequately protected. Technology companies and software developers like Microsoft have established new industry standards by improving the security of their products

---

[21] Cal. Exec. Order No. B-34-15 (Aug. 31, 2015).

[22] Russell Brandom, *Congress Passes Controversial Cybersecurity Bill Attached to Omnibus Budget*, THE VERGE (Dec. 18, 2015, 12:08 PM), http://www.theverge.com/2015/12/18/10582446/ congress-passes-cisa-surveillance-cybersecurity.

[23] Andy Greenberg & Yael Grauer, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 5:30 PM), http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws.

[24] *Id.*

through private investment and research.[25] By the same token, government regulation has also proved valuable in requiring corporations to disclose security breaches to their customers and permitting judicial review of companies who carelessly handle customers' confidential information.[26] Increasing federal prosecution and punishment of hackers under the CFAA and other broad statutes targets mostly petty crimes as opposed to massive attacks perpetrated by foreign hackers. A stronger CFAA would not have prevented the Sony hack, but a thorough risk assessment strategy and a less permeable database fortified with encryption would have greatly reduced the effectiveness of the attack.[27]

The argument proceeds in five parts. Part II explores the Sony hack in detail. Part III analyzes the hack's chilling impact on the entertainment community and freedom of expression. Part IV assesses the effectiveness of existing public and private resources in deterring cyber attacks. Part V proposes solutions to bolster cyber security for everyone and preserve free speech in an increasingly transparent world. Part VI concludes.

## II. THE SONY HACK SAGA

On the morning of November 24, 2014, thousands of Sony employees discovered a sinister message on their computer screens from the "Guardians of

---

[25] *Security Development Lifecycle*, ACCUVANT (2016), http://www.accuvant.com/labs/sdl.

[26] SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS 235 (Cambridge Univ. Press, 2014).

[27] John Gaudiosi, *Why Sony Didn't Learn from Its 2011 Hack*, FORTUNE (Dec. 24, 2014, 1:22 PM), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack.

Peace."[28] It read, "We've obtained all your internal data including your secrets and top secrets" and threatened a worldwide release if the studio failed to act as the hackers instructed.[29] On December 8, 2014, the hackers commanded Sony to "stop immediately showing the movie of terrorism which can break the regional peace and cause the War."[30] That "movie of terrorism" was *The Interview* and it triggered considerable controversy long before the hack surfaced.

### *A. The Inception of The Interview and Initial Stages of the Hack*

Seth Rogen originally envisioned the film's plot while starring in the *Green Hornet*, an action-comedy featuring the son of a renowned journalist who fights crime to avenge his father's death.[31] Rogen also admired the movie *Borat*, which featured a journalist sent to the U.S. by the government of Kazakhstan to report on American culture.[32] A combination of both pictures inspired Rogen's idea to create a movie about a journalist interviewing someone infamous with the CIA pulling strings.[33] Rogen and his production company partner Evan Goldberg pitched the idea to Sony executives and Sony

---

[28] Jose Pagliery, *The Sony Mega-Hack: What You Need to Know*, CNN (Dec. 12, 2014, 11:13 AM), http://money.cnn.com/2014/12/09/technology/security/sony-hacking-roundup.

[29] *Id.*

[30] *Id.*

[31] Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 28, 2015, 9:27 PM), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

[32] *Borat: Cultural Learnings [sic] of America for Make Benefit Glorious Nation of Kazakhstan*, IMDB (2006, 9:28 PM), http://www.imdb.com/title/tt0443453/synopsis?ref_=ttpl_pl_syn.

[33] Seal, *supra*.

Pictures Chairman Amy Pascal reportedly loved the script.[34] She was in good company. When the movie test-screened in March of 2014, the audience responded positively and the studio's executives were thrilled.[35]

The first sign of trouble arose in June of 2014 when Sony released a teaser trailer of *The Interview*. Almost immediately, the North Korean government blasted the U.S. for allowing Sony to publish a film it considered an act of terrorism.[36] Alarmed by this reaction, Sony Corporation Chairman Kazuo Hirai encouraged Sony Pictures to soften the film, including the final scene where Kim Jong-un's head violently explodes.[37] Over Rogen's objections, Sony made the change and censored several other scenes.[38] Sony also contacted Rich Klein at McLarty Associates, an international business advisory firm, who assured them a physical strike to the U.S. was beyond North Korea's capabilities.[39] Nonetheless, Sony insisted on removing its name from all promotional materials and slowing the film's social media marketing campaign.[40]

To Sony's despair, these attempts to pacify North Korea were fruitless. North Korea sent numerous threats to Sony executives attempting to extort the

---

34 Seal, *supra*.
35 *Id.*
36 *Id.*
37 *Id.*
38 *Id.*
39 *Id.*
40 *Id.*

studio to cancel *The Interview* or be "bombarded as a whole."[41] In July, the hackers began constructing malicious software that infiltrated Sony's servers and gradually stole massive amounts of data.[42] The hackers then firebombed Sony's servers and released a total of 100 terabytes of data in eight total dumps taking place over the next two weeks.[43]

### *B. The Hack Surfaces and Exposes Massive Amounts of Data*

A day after releasing the ominous warning on November 24, 2014, the hackers leaked four copies of unreleased Sony movies on pirate websites.[44] According to Excipio, a company that specializes in detecting Internet copyright infringement, *Fury*, starring Brad Pitt, was downloaded more than 2.3 million times and *Annie*, starring Jamie Foxx, was downloaded more than 278,000 times, depriving Sony of millions of dollars from prospective box office sales.[45] Additionally, copies of *Mr. Turner*, *Still Alice* and the script of *Spectre*, the next James Bond film, were released.[46]

Furthermore, the social security numbers and birthdays of 47,426 Sony employees and contractors, including Conan O'Brien and Sylvester Stallone,

---

[41] Jose Pagliery, *The Sony Mega-Hack: What You Need to Know*, CNN (Dec. 12, 2014, 12:50 PM), http://money.cnn.com/2014/12/09/technology/security/sony-hacking-roundup.
[42] *Id*.
[43] Seal, *supra*.
[44] Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 28, 2015, 9:27 PM), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.
[45] Jose Pagliery, *"Sony-pocalypse: Why the Sony Hack is One of the Worst Hacks Ever*, CNN (Dec. 29, 2014, 10:01 AM), http://money.cnn.com/2014/12/04/technology/security/sony-hack.
[46] Jose Pagliery, *The Sony Mega-Hack: What You Need to Know*, CNN (Dec. 12, 2014, 5:20 PM), http://money.cnn.com/2014/12/09/technology/security/sony-hacking-roundup.

became public.[47] Soon after, multiple employees learned identity thieves were using their credit cards and bank information.[48] On December 5, 2014, employees' handheld devices and personal computers were hacked with a message commanding them to publicly denounce *The Interview* or risk their family's safety.[49]

The hackers were relentless. On December 16, 2014, they threatened an attack reminiscent of September 11, 2001 if Sony failed to pull *The Interview*.[50] The threat drew the attention of the U.S. Department of Homeland Security, which concluded there was no credible evidence of a plot to inflict physical violence against Sony or movie theaters scheduled to premiere the film.[51] Nevertheless, major theater chains backed out and Sony canceled the Christmas Day release.[52] It was not until President Obama and a sizable portion of the American public expressed disappointment in Sony's decision to pull the picture and capitulate to the hackers' demands that Sony reinstated the premiere.[53] *The Interview* opened online the morning of December 24, 2014, and earned forty million dollars in online sales, making it the best-selling

---

47 Pagliery, *supra* note 46.
48 Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 28, 2015, 1:10 PM), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.
49 *Id.*
50 *Id.*
51 *Id.*
52 *Id.*
53 *Id.*

online release of all time.[54] On Christmas Day, the film premiered in mostly independent theaters nationwide.[55]

### *C. The Embarrassing Aftermath*

Although the physical threats against Sony and its employees never materialized, the "Guardians of Peace" unleashed irreparable damage. On December 8, 2014, the hackers released thousands of employee work emails, including those from the desks of Sony Screen Gems President Clint Culpepper and Sony Pictures Chairman Amy Pascal.[56] In an email to Pascal, Culpepper was caught calling Kevin Hart a "whore" for seeking additional compensation to tweet support of his upcoming movies with Sony.[57] A email thread between Pascal and *Moneyball* producer Scott Rudin turned scandalous when Pascal asked Rudin what she should ask President Obama at a breakfast fundraiser. Pascal suggested a question about *Django Unchained* and Rudin replied with *12 Years a Slave*.[58]

Perhaps the most infamous of the leaked emails was a heated exchange between Pascal and Rudin over Angeline Jolie's insistence on using director David Fincher for her movie *Cleopatra* while Rudin sought Fincher for the Steve Jobs biopic. In response to Pascal's inability to convince Jolie to use

---

54 Seal, *supra* note 48.
55 *Id.*
56 *Id.*
57 William Boot, *Shocking New Reveals From Sony Hack*, THE DAILY BEAST (Dec. 12, 2014, 4:00 PM), http://www.thedailybeast.com/articles/2014/12/12/shocking-new-reveals-from-sony-hack-j-law-pitt-clooney-and-comparing-fincher-to-hitler.html.
58 Matthew Zeitlin, *Scott Rudin on Obama's Favorite Movies: "I Bet He Likes Kevin Hart*," BUZZFEED (Dec. 10, 2014, 1:15 PM), http://www.buzzfeed.com/matthewzeitlin/scott-rudin-on-obama-i-bet-he-likes-kevin-hart#.hdmO0Ax4j.

someone other than Fincher, Rudin called Jolie a "camp event" and a "minimally talented spoiled brat."[59] Oddly, the media held Pascal responsible for Rudin's insults, and she immediately apologized to Jolie shortly after the emails were exposed. It was one of many apologies on Pascal's task list after she criticized director Cameron Crowe's *Aloha* set in Hawaii, slammed writer Aaron Sorkin for charging an "insane fee" on *Flash Boys* and suggested that Sorkin might be sleeping with Molly Bloom while adapting her memoirs for the film *Molly's Game*.[60] In the end, Pascal could not withstand the storm and was fired in February of 2015.[61]

The most sensitive emails did not hit the tabloids. Those emails include a Sony employee shopping for Ritalin, another employee discussing her difficulty achieving pregnancy and other personal communication with no place in the public sphere.[62] The intimate correspondence between employees was largely unexplored until websites like WikiLeaks organized hundreds of thousands of private documents, emails and financial information into a user-

---

[59] Laura Italiano, *Producer: Jolie a "Spoiled Brat" from "Crazyland*," PAGE SIX (Dec. 11, 2014, 8:10 AM), http://pagesix.com/2014/12/11/producer-blasts-angelina-in-hacked-sony-e-mails.

[60] William Boot, *Shocking New Reveals From Sony Hack*, THE DAILY BEAST (Dec. 12, 2014, 4:00 PM), http://www.thedailybeast.com/articles/2014/12/12/shocking-new-reveals-from-sony-hack-j-law-pitt-clooney-and-comparing-fincher-to-hitler.html.

[61] Jake Coyle, *Amy Pascal, Ex-Sony Chief, Acknowledges She Was Fired*, HUFFINGTON POST (Feb. 12, 2015, 9:24 AM), http://www.huffingtonpost.com/2015/02/12/amy-pascal-fired_n_6673222.html.

[62] Brian Barrett. *The Sony Hacks are Goddamn Terrifying*, GIZMODO (Dec. 9, 2014, 9:50 AM), http://gizmodo.com/the-sony-hacks-are-goddamn-terrifying-1668911102.

friendly database for anyone to search.[63] Sony claimed it owned the copyright to these files and forbade the media from disseminating the information.[64] However, as explained in Part IV, it is doubtful Sony owns the copyright and would therefore have no standing to sue.[65] Plus, given its history releasing confidential documents contrary to American law,[66] WikiLeaks is unlikely to comply with Sony's pleas regardless of their validity.

## III. THE HACK'S CHILLING IMPACT ON PRIVACY AND FREE SPEECH

The First Amendment forbids Congress from abridging the freedom of speech.[67] This prohibition was later extended to state governments via the Doctrine of Incorporation[68] and, in some states, to privately owned places of public accommodation.[69] The First Amendment, however, does not sanction private parties for chilling private speech. Of course, the federal government

---

[63] Andrea Mandell & Elizabeth Weise, *Wikileaks Dumps Even More Sony Files*, USA TODAY (June 19, 2015, 1:05 PM), http://www.usatoday.com/story/life/movies/2015/06/18/sony-hack-nightmare-continues-wikileaks/28931105.

[64] Michael Cieply & Brooks Barnes, *Sony Pictures Demands that News Agencies Delete 'Stolen Data,'* N.Y. TIMES (Dec. 14, 2014), http://www.nytimes.com/2014/12/15/business/sony-pictures-demands-that-news-organizations-delete-stolen-data.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=1.

[65] *See infra* Part IV.C.

[66] Frances Romero, *The Wikileaks War Logs*, TIME (Nov 29, 2010), http://content.time.com/time/specials/packages/article/0,28804,2006558_2006562_2006567,00.html.

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

[68] Gitlow v. N.Y., 268 U.S. 652, 660 (1925) (finding "the freedom of speech and of the press. . . are among the fundamental personal rights and liberties protected by the due process clause of the Fourteenth Amendment from impairment by the States.").

[69] PruneYard Shopping Ctr. v. Robins, 447 U.S. 74, 87 (1980) (holding the California Constitution permitting individuals to petition at privately owned mall open to the public did not violate mall owner's First Amendment rights since the views expressed by visitors would not likely be identified with those of the owner and the owner was free to disassociate himself from those views).

can prosecute computer fraud via the CFAA, and several states have recognized the unauthorized publication of private facts as an actionable tort.[70] But even if every hacker is jailed and every snoop sanctioned, the mere possibility of surveillance and disclosure is enough to chill everyday speech.[71]

### *A. The Abolition of Privacy in a Technologically Dependent World*

In a landmark editorial for *The New York Times* titled "Hacking Our Humanity," Frank Bruni declared that the Sony hack officially obliterated the assumption that digital private information will stay confidential.[72] This applies not just to studio executives or blockbuster celebrities but everyone who uses digital means to communicate or store information. After all, if the media-giant Sony's servers could be looted, no one is safe. Corporations and search engines routinely monitor activity online, employers track current and prospective employees' virtual footprints, mysterious stalkers and identity thieves have an endless depository of information at their disposal, and even the federal government spies on its own citizens.[73]

These trends have not gone unnoticed. According to a Pew Research Center survey from November of 2014, Americans under sixty-five have expressed the most concern over the privacy of email correspondence in the

---

[70] *Publication of Private Facts*, DIGITAL MEDIA LAW PROJECT (Dec. 12, 2015, 4:26 PM), http://www.dmlp.org/legal-guide/publication-private-facts.

[71] *See infra* Part III.A-D.

[72] Frank Bruni, *Hacking Our Humanity*, N.Y. TIMES (Dec. 20, 2014, 9:53 PM), http://www.nytimes.com/2014/12/21/opinion/sunday/frank-bruni-sony-security-and-the-end-of-privacy.html.

[73] *Timeline of NSA Domestic Spying*, ELECTRONIC FRONTIER FOUND. (2015), https://www.eff.org/nsa-spying/timeline.

wake of various corporate data breaches and Edward Snowden's revelations of widespread government surveillance.[74] Younger citizens have become increasingly more dependent on technology considering the massive roles social media, email and smartphones play in the lives of youth. Almost every American teen and young adult uses email, Facebook or text messaging to communicate with the outside world.

Thus, even though 81% of social media users feel uncomfortable sharing private information, 59% of texters are wary about the security of their messages and 57% of those with email accounts question the confidentiality of their correspondence,[75] only a microscopic minority is reducing its dependence on these mediums.[76] Even the most concerned citizen would be taking drastic measures to terminate his or her social media accounts given the tremendous value such services provide in maintaining hundreds of personal and professional connections. Moreover, except for those living in Amish communities, dispensing with email is an unimaginable proposition that would make it virtually impossible to accomplish anything in a timely manner.

---

[74] Mary Madden, *Public Perception of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014, 9:50 PM) (finding 59% of adults under 65 to consider email contents "very sensitive" compared to 42% of seniors) http://www.pewinternet.org/2014/11/12/public-privacy-perceptions.

[75] *Id.*

[76] Sara Radicato & Quoc Hoang, *Email Statistics Report, 2011-2015*, RADICATI GRP. (May 2011), *available at* http://www.pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf (projecting worldwide email accounts to increase from 3.1 billion in 2011 to nearly 4.1 billion in 2015 and social networking accounts to increase from 2.4 billion in 2011 to 3.9 billion in 2015).

Although dependence on technology has not diminished despite growing concerns of cyber security, there has been a disturbing trend of tailoring virtual communication to comport with societal standards. A 2013 survey by the PEN American Center, a prominent organization of literary writers, revealed 28% of its members have curtailed activity on social media, 24% have avoided certain topics in phone calls or email, and 16% have abandoned ideas to write or speak on a particular topic in fear of angering the government.[77] For example, PEN member and literary biographer Charles J. Shields said he canned a project exploring civil defense in the U.S. because it dealt with dirty bombs and mass casualties.[78]

### *B. The Merger of Privacy and Speech*

Currently courts nationwide are grappling over whether the Fourth Amendment's prohibition against unreasonable searches and seizures shields digital data from unauthorized government appropriation[79] and have largely overlooked the First Amendment's free speech guarantee. In the poetic words of former Associate U.S. Supreme Court Justice Lewis Brandeis, the "freedom

---

[77] *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN AM. CTR. (Nov. 12, 2013), *available at* http://www.pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling %20Effects%20w%20Color%20cover-UPDATED.pdf.

[78] Noam Cohen, *Surveillance Leaves Writers Wary*, N.Y. TIMES (Nov. 11, 2013), http://www.nytimes.com/2013/11/12/books/pen-american-center-survey-finds-caution-among-members.html.

[79] Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015) (holding plaintiff telephone service subscribers in class action suit failed to show substantial likelihood NSA bulk data collection policy was unreasonable in vacating preliminary injunction); *In Re: Application for Telephone Information Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) (holding the government must obtain a court order before obtaining historical cell phone location data because users have a reasonable expectation of privacy in the location of their phones).

to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth."[80] This freedom to think, a freedom essential to the freedom of speech, cannot be realized without some privacy of thought. As Jeremy Bentham's *Panopticon Writings*[81] and George Orwell's *1984*[82] vividly illustrate, knowledge of the mere possibility of surveillance greatly impacts behavior.

Neil Richards, a professor at Washington University School of Law in St. Louis and internationally renowned expert in exploring the interplay between privacy, free speech and cyberspace, examines how technology has rendered cherished civil liberties dangerously vulnerable. Although digital platforms have been an undeniable force for good, enabling anyone with a computer to access endless knowledge and communicate worldwide instantaneously, they create data trails revealing society's most intimate thoughts and desires.[83] Email providers store all correspondence and data clouds retain every uploaded document.[84] Facebook and other social media networks document millions of digital diaries for the world to read.[85] Search

---

[80] Whitney v. California, 274 U.S. 357, 375 (1927) (overruled on other grounds by Brandenburg v. Ohio, 395 U.S. 444 (1969)).

[81] JEREMY BENTHAM, THE PANOPTICON WRITINGS Preface (1843) (lauding the Panopticon structure as "a new mode of obtaining power of mind over mind, in a quantity hitherto without example").

[82] GEORGE ORWELL, 1984 11 (1949) (introducing the concept of Thoughtcrime as something "you might dodge successfully for a while, even for years, but sooner or later they were bound to get you").

[83] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 2 (2015).

[84] *Id.* at 3.

[85] *Id.*

engines compile records of Internet users' wonderings, musings and fantasies, much of which many users would prefer to keep private.[86]

As a result, to develop new ideas and original speech, society must first safeguard the process of intellectual exploration and belief formation in digital mediums to provide a meaningful guarantee of intellectual privacy.[87] Considering the vast majority of human interaction presently occurs via some form of technology, bolstering cyber security is a prerequisite to protecting the right to free speech from digital degradation.

### *C. The Entertainment Industry Vindicates First Amendment Freedoms*

The entertainment industry at large derives its power from the nation's robust tradition of free speech and expression. Some of the greatest movies ever made sharply challenge existing governments and ways of life. For instance, *The Wizard of Oz* used fanciful symbolism to mask a harsh critique of the nation's economic, political and social status in the late nineteenth century.[88] *Schindler's List* revealed the unspeakable horrors of Nazi fascism,[89] and *12 Angry Men* unveiled the danger racism poses to the legal system.[90]

Undoubtedly, *The Interview* is not one of the greatest films ever made. A slapstick and crass comedy, the movie is tough to take seriously.

---

[86] Richards, *supra* note 83.

[87] *Id.* at 5.

[88] Sara Silverstein, *The Real, Forgotten Meaning of* The Wizard of Oz, YAHOO (2015, 10:10 PM), https://screen.yahoo.com/heres-real-forgotten-meaning-wizard-040000330.html.

[89] *Schindler's List Plot Overview*, SPARKNOTES (2016), http://www.sparknotes.com/film/schindlerslist/summary.html.

[90] *12 Angry Men Full Synopsis*, TURNER CLASSIC MOVIES (2016), http://www.tcm.com/tcmdb/title/94081/12-Angry-Men/full-synopsis.html.

Nevertheless, Lee Min-bok, a North Korean defector and advocate for free speech, imported thousands of copies of the film into his home country via air balloon, illustrating the vital role cinema plays in vindicating First Amendment freedoms.[91] *The Interview's* ridicule of Kim Jong-un and the destitute country he imprisons falls squarely within the most coveted crevasse of the First Amendment: political speech or speech critiquing existing governments, politicians and cultures. In North Korea, such speech is punishable by death.[92] In the U.S., political speech is celebrated and the lifeblood of democracy. Thus, North Korea's attempt to silence this speech through cyber terrorism constitutes an attempt to undermine the very foundation of freedom on which the U.S. was built. Unfortunately, this attempt was somewhat successful.

### *D. Censorship of The Interview Eviscerates First Amendment Rights*

*The Interview* ultimately reached the public as scheduled the morning of December 24, 2014, online and in independent theaters nationwide. However, the released film was watered down considerably to assuage the hackers. For example, editors removed significant amounts of blood and gore from a scene featuring a fight with North Korean soldiers.[93] Sony also removed its name from the credits and all promotional materials in fear of further

---

[91] Paula Hancocks, *Defector Sends Thousands of* The Interview *DVDs to North Korea*, CNN (Apr. 11, 2015, 10:14 PM), http://www.cnn.com/2015/04/07/asia/north-korea-interview-balloons.

[92] *Id.*

[93] William Boot, *Sony Emails Show How the Studio Plans to Censor Kim Jong-Un Assassination Comedy* The Interview, THE DAILY BEAST (Dec. 15, 2014, 3:25 PM), http://www.thedailybeast.com/articles/2014/12/15/exclusive-kim-jong-un-assassination-comedy-the-interview-will-allegedly-be-censored-abroad.html.

infuriating the hackers.[94] Furthermore, the scene of Kim Jong-un's assassination was changed from showing his head explode to a clean shot of his head quickly obscured by flames.[95] Whether it is more enthralling to watch a man's head explode or be enveloped by fire is irrelevant. Sony's decision to censor its speech to calm the hackers, while enraging mega-star Seth Rogen who insisted on preserving the gory details, tributes the power of cyber terrorism in silencing unfavorable viewpoints.

## IV. EXISTING METHODS TO DETER CYBER TERRORISM

It is one thing to illustrate the problem of cyber terrorism but another to propose an effective solution. To its credit, the federal government has built a sizable arsenal of weapons to prosecute hackers and limit the exposure of confidential information via the Computer Fraud and Abuse Act (CFAA), Racketeer Influenced and Corrupt Organizations Act (RICO) and Digital Millennium Copyright Act (DMCA). Additionally, the federal government has encouraged information sharing between the private and public sector to combat cyber terror collectively through the Cybersecurity Information Sharing Act (CISA). Many state governments, including California's, have done the same. However, although each of these strategies has benefits, all of them have proven ineffective in significantly curtailing cyber terrorism, preserving privacy and liberating speech.

---

[94] William Boot, *Shocking New Reveals from Sony Hack*, THE DAILY BEAST (Dec. 12, 2014, 10:15 PM), http://www.thedailybeast.com/articles/2014/12/12/shocking-new-reveals-from-sony-hack-j-law-pitt-clooney-and-comparing-fincher-to-hitler.html.

[95] *Id.*

### *A. The Computer Fraud and Abuse Act (CFAA)*

The CFAA is designed to criminalize the unauthorized access to a computer.[96] Unsurprisingly, the Act prohibits hacking into government computers,[97] disclosing information pertaining to national security,[98] using information for fraudulent purposes,[99] trafficking passwords,[100] transmitting viruses[101] and initiating extortion.[102] However, the teeth of the statute rest within 18 U.S.C. § 1030(a)(2)(C), which prohibits intentionally accessing a computer without authorization or exceeding authorized access and thereby obtaining information from that computer. Under the Commerce Clause, the federal government via the CFAA may regulate any computer affecting interstate commerce.[103] Undoubtedly, Sony's extensive database affected interstate commerce[104] and the hackers intentionally accessed those computers and thereby obtained information they then leaked to the Internet. Theoretically, this section of the statute could be used to hold the hackers accountable. Practically, it is wishful thinking.

---

[96] Margaret Rouse, *Computer Fraud and Abuse Act (CFAA)*, TECHTARGET (June 2012), http://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA.

[97] 18 U.S.C. § 1030(a)(3) (1986).

[98] 18 U.S.C. § 1030(a)(1) (1986).

[99] 18 U.S.C. § 1030(a)(4) (1986).

[100] 18 U.S.C. § 1030(a)(6) (1986).

[101] 18 U.S.C. § 1030(a)(5) (1986).

[102] 18 U.S.C. § 1030(a)(7) (1986).

[103] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1568 (2010); 18 U.S.C. § 1030(e)(2)(B) (defining protected computers as those "used in or affecting interstate or foreign commerce or communication).

[104] Orin S. Kerr, *Does the Federal Computer Hacking Law Apply to a Laptop Not Connected to the Internet?* WASH. POST (Aug. 25, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/08/25/does-the-federal-computer-hacking-law-apply-to-a-laptop-not-connected-to-the-internet/ (conceding the CFAA is so broad that it includes almost every computer, even if offline).

Even in the rare case where law enforcement is able to identify the source of foreign cyber attacks, the chances of actual prosecution are slim to none.[105] No one seriously contends the U.S. will indict Kim Jong-un despite his government's involvement with the hack. Organizations of hackers in Russia and Ukraine have been linked to Target and Home Depot data breaches,[106] but no rational prosecutor could expect either country to corral the culprits for extradition given the absence of an extradition treaty between those nations and the U.S.[107] In May of 2014, the Department of Justice (DOJ) indicted five Chinese officers for launching an eight-year espionage campaign hacking into the computers of six major American companies to steal trade secrets.[108] To this day, China has turned the other cheek.[109] Since the CFAA's inception in 1984, the DOJ has opened an average of eighty cases each year despite countless CFAA violations worldwide.[110] In sum, the CFAA is largely powerless outside America's borders.

1. Bolstering the CFAA Will Not Deter Professional Hackers

President Obama seeks to bolster the CFAA's sanctions claiming it will more effectively deter cyber terrorism.[111] As written, the Act punishes a

---

[105] Shawn Tuma, *Will Changes to the CFAA Deter Hackers?* DARK MATTERS (Feb. 3, 2015, 2:22 PM), http://darkmatters.norsecorp.com/2015/02/03/will-changes-to-the-cfaa-deter-hackers.
[106] *Id.*
[107] 18 U.S.C. § 3181.
[108] Tuma, *supra*.
[109] *Id*.
[110] *Obama Proposes-Cyber Law Update in Wake of Sony Hack*, RUSSIA TODAY (Jan. 13, 2015, 10:14PM), https://www.rt.com/usa/222327-obama-cyber-cfaa-blake/.
[111] Orin S. Kerr, *Obama's Proposed Changes to Computer Hacking Statute: A Deep Dive*, WASH. POST (Jan. 14, 2015, 10:21 PM), https://www.washingtonpost.com/news/volokh-

Section 1030(a)(2)(C) violation with a maximum of one-year imprisonment for the first offense.[112] However, if the hack was conducted to gain a commercial advantage in furtherance of a tortious act impacting information valued above $5,000, the penalty rises to a maximum of five years imprisonment.[113] President Obama seeks to increase the penalties to three and ten years respectively.[114]

In practice, this will do nothing to deter large scale attacks like Sony's because those qualify as more serious offenses under Section 1030(5), which covers damaging a hacked computer and Section 1030(7), which prohibits using information obtained in a hack to conduct extortion. Those who engage in hacks on this level are ready to accept the small risk of spending decades in prison if caught in exchange for reaping valuable fruits of the crime.[115] However, although bolstering the penalties will not change the behavior of professional hackers, it may sack relatively trivial conduct with life-changing consequences.[116]

---

conspiracy /wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive.

[112] 18 U.S.C. § 1030(c)(2)(A) (1986).

[113] 18 U.S.C. § 1030(c)(2)(B)(III) (1986).

[114] Kerr, *supra*.

[115] Chris Strohm, *Cybercrime Remains Growth Industry with $445 Billion Lost*, BLOOMBERG BUS. (June 9, 2014, 6:57AM), http://www.bloomberg.com/news/articles/2014-06-09/cybercrime-remains-growth-industry-with-445-billion-lost; *Cyberterrorism Driven Mostly by Money*, INDO-ASIAN NEWS SERV. (December 17, 2015, 1:46PM), http://www.india.com/news/world/ cyberterrorism-driven-mostly-by-money-792428/.

[116] *See infra* Part IV.A.2.

2. "Aaron's Law" and the Overbroad CFAA

In 2011, 25-year-old Aaron Swartz was charged with eleven violations of the CFAA and two counts of wire fraud for downloading academic journal articles from JSTOR through the Massachusetts Institute of Technology's computer network and disseminating them to the public for free.[117] Swartz faced thirty-five years in prison and a possible fine of $1 million.[118] Although the prosecution agreed to reduce the sentence to six months and waive the fine, Swartz rejected the plea and ultimately committed suicide before trial.[119] As a result of Aaron's passing, Congressman Zoe Lofgren, Senator Ron Wyden and Senator Rand Paul reintroduced "Aaron's Law" in April of 2015 as a revision to a 2013 proposal, which would restrict the CFAA to criminalizing circumvention of technological safeguards and disallow compound sentencing.[120]

Swartz's indictment included counts under Section 1030(a)(4) and Section 1030(a)(5), both relatively serious violations of the CFAA, which cover hacks that perpetrate fraud and cause damage, respectively. However, the indictment was filled with violations of Section 1030(a)(2), which as

---

[117] Kevin Cullen & John R. Ellement, *MIT Hacking Case Lawyer Says Aaron Swartz was Offered Plea Deal of Six Months Behind Bars*, BOSTON GLOBE (Jan. 14, 2013, 5:10 PM), http://www.boston.com/metrodesk/2013/01/14/mit-hacking-case-lawyer-says-aaron-swartz-was-offered-plea-deal-six-months-behind-bars/hQt8sQI64tnV6FAd7CLcTJ/story.html.

[118] *Id.*

[119] *Id.*

[120] *Wyden, Lofgren, Paul Introduce Bipartisan, Bicameral Aaron's Law to Reform Abused Computer Fraud and Abuse Act*, OFFICE OF SENATOR RON WYDEN (Apr. 21, 2015, 9:29 PM), https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-.

referenced above, prohibits intentionally accessing a computer without authorization or in excess of authorization and thereby obtaining information. The term "exceeding authorization" is defined in Section 1030(e)(6) as accessing a computer with authorization and using such authorization to obtain or alter information in the computer that the suspect is not entitled to obtain or alter.[121]

Therefore, an employee who uses a company computer at work to check sports scores or receives a personal email without permission violates the CFAA because he or she is obtaining information without entitlement. In 2009, the Ninth Circuit ruled violations of company policy do not trigger the CFAA[122] and a California district court has held the mere breach of an online service provider's terms of use is not actionable under the CFAA.[123] However, the U.S. Supreme Court has yet to endorse these narrow interpretations and the breadth of Section 1030(a)(2) remains in considerable dispute.[124]

### *B. The Racketeer Influenced and Corrupt Organizations Act (RICO)*

RICO is another weapon at the federal government's disposal to combat cyber terrorism. The Act prohibits anyone employed by or associated with an enterprise engaged in interstate or foreign commerce to conduct or

---

[121] 18 U.S.C. § 1030(e)(6) (1986).

[122] U.S. v. Nosal, 676 F.3d 854 (9th Cir. 2012).

[123] U.S. v. Drew, 259 F.R.D. 449, 468 (C.D. Cal. 2009) (holding a misdemeanor conviction under the CFAA based on defendant's intentional violation of MySpace's terms of use violates the void-for-vagueness doctrine).

[124] Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015), http://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/.

participate in the enterprise's racketeering activity.[125] The Patriot Act added Section 1030(a)(1) to the CFAA, which sanctions hacks that compromise national security, and Section 1030(a)(5), which sanctions hacks that damage a protected computer, to the long list of racketeering activities.[126] RICO violations carry large sanctions upwards of twenty years to life but require some pattern of racketeering activity and an enterprise engaged in interstate or foreign commerce.[127] As a result, RICO can be effective when prosecuting sophisticated attacks conducted by a group of domestic hackers but has little ability to reach foreign cyber terrorists in nations without extradition agreements and lone wolves who wreck havoc.

### *C. The Digital Millennium Copyright Act (DMCA)*

The DMCA is a reactive measure to limit the damage of a cyber attack by requiring websites that post appropriated material to promptly remove it at the request of the victim by claim of copyright.[128] The catch, however, is that the request must be made by the company or individual that owns the copyright to the material in question or someone authorized to act on the copyright owner's behalf.[129] For example, Jennifer Lawrence invoked the DMCA to stop

---

[125] 18 U.S.C. § 1962(c) (1970).

[126] OFFICE OF LEGAL EDUCATION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 15 (2011), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[127] Ave Mince-Didier, *Federal RICO Laws*, CRIMINAL DEFENSE LAWYER (2016), http://www.criminaldefenselawyer.com/crime-penalties/federal/rico-offenses.htm.

[128] 17 U.S.C. § 512(c)(1)(C) (1998).

[129] 17 U.S.C. § 512(c)(3)(A)(vi) (1998).

Google from linking to her stolen nude photographs.[130] Since Lawrence owns the copyright to her photos, there was no question the DMCA was properly at her disposal. In contrast, companies whose servers are breached may not own the copyright to the purloined data. For example, in 2004 a California district court held that Diebold, a manufacturer of electronic voting machines, did not possess the copyright to leaked internal documents revealing flaws in its machines and was therefore unable to use the DMCA to remove the documents from the Internet.[131] Furthermore, the court found it was unreasonable for Diebold to believe it owned the copyright to incriminating employee emails just because it operated the database through which the emails were transmitted.[132]

Likewise, a court could find Sony has no copyright to emails or data stored on its servers. As a result, Sony's pleas to various websites to refrain from posting material revealed in the hack have mostly fallen on deaf ears. At present, WikiLeaks operates a user-friendly and searchable database containing approximately 30,000 internal documents and 170,000 employee emails exposed by the hack.[133]

---

[130] Alex Fitzpatrick, *Here's How Celebs Can Get Their Nude Selfies Taken Down*, TIME (Sep. 2, 2014, 4:18 PM), http://time.com/3256732/jennifer-lawrence-selfies-copyright.

[131] Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

[132] *Id.* at 1204.

[133] Russell Brandom, *Wikileaks Has Published the Complete Sony Leaks in a Searchable Database*, THE VERGE (Apr. 16, 2015, 2:25 PM), http://www.theverge.com/2015/4/16/8431497/wikileaks-sony-hack-emails-north-korea-julian-assange.

### *D. The Cybersecurity Information Sharing Act (CISA)*

A more collaborative solution to combat cyber terror is to ally the government and private sector by encouraging the sharing of information related to cyber security threats. CISA grants legal immunity to companies that share data with the federal government for the purpose of prosecuting and preventing cyber attacks.[134] One of the most controversial aspects of the law is an exemption from the Freedom of Information Act (FOIA), which would require the federal government to inform the public upon request when a corporation oversteps and shares irrelevant personal information.[135] Normally, the government cannot access someone's personal information absent probable cause and a warrant as required by the Fourth Amendment.[136] However, these protections do not apply if information is shared with a third party because the act of sharing surrenders any reasonable expectation of privacy in the data.[137]

Privacy advocates nationwide decry CISA as incentivizing companies to betray users and share massive amounts of intimate information with the

---

[134] Lizzy Finnegan, *CISA and the War on Privacy*, BREITBART (Nov. 10, 2015), http://www.breitbart.com/tech/2015/11/10/cisa-and-the-war-on-privacy.

[135] *Id.*

[136] U.S. CONST. amend. IV. (declaring "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause. . .").

[137] U.S. v. Miller, 425 U.S. 435, 443 (1976) (holding "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the defendant] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

government without a warrant.[138] In one week of action, CISA's opponents sent six million faxes to various senators urging them to vote against the bill.[139] CISA's proponents, including IBM, Facebook, Intel and other major technology companies,[140] argue the law's loophole requiring companies withhold information they know contains sensitive data is sufficient to protect user privacy. However, this provision lowers the standard from a previous version of the law that prohibited the sharing of information companies reasonably believe contains sensitive information.[141]

CISA recently passed in December 2015, so it remains to be seen whether the law will effectively prevent cyber attacks. Nevertheless, the impact of mass government surveillance achieved via information sharing will still chill free expression in virtual mediums. For many, the fear of private communication landing in the hands of a malicious hacker remains constant if a federal or state government official examines the communication instead.[142] Although a categorical ban on information sharing is unwise since much can be

---

[138] Andy Greenberg & Yael Grauer, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 8:50 AM), http://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws.

[139] Lee Tien, *Amendments to CISA "Cybersecurity" Bill Fail in All Regards*, ELECTRONIC FRONTIER FOUND. (Sept. 1, 2015, 10:20 AM), https://www.eff.org/deeplinks/2015/09/amendments-cisa-cybersecurity-bill-fail-all-regards.

[140] *Stop CISA*, FIGHT FOR THE FUTURE (2015), http://www.decidethefuture.org.

[141] Tien, *supra* note 116.

[142] April Glaser, *Academics and Researchers Against Mass Surveillance*, ELECTRONIC FRONTIER FOUND. (Feb. 12, 2014), https://www.eff.org/deeplinks/2014/02/academics-and-researchers-against-mass-surveillance (reasoning that when people know the government is collecting data from their telephone calls, emails and text messages, they will adjust their communication accordingly).

learned through teamwork,[143] a more balanced approach is warranted. For instance, a CISA amendment that prohibits the sharing of certain kinds of personal data absent exigent circumstances and eliminates the FOIA exemption to allow government accountability through public review can more effectively protect user privacy and still provide law enforcement a powerful weapon to proactively combat cyber terror.

## V. SOLUTIONS TO BOLSTER CYBER SECURITY AND PROTECT FREE SPEECH

Cyber security is indispensible to protecting individual privacy in media without which a user's speech in virtual mediums will be inevitably chilled for fear of surveillance and public disclosure. However, cyber security is underproduced by the private sector because it is non-excludable in that everyone can use it and non-rivalrous in that it can be consumed simultaneously.[144] Thus, government regulation is warranted to incentivize the private sector to enhance cyber security by rewarding those who adequately protect customer data while exposing others to liability for leaving customers vulnerable.[145] By the same token, private companies can improve security on their own by developing advanced software to bolster their defenses, enlisting

---

[143] V. Gerard Comizio, *Information Sharing is Key to Avoiding a Cyberattack*, TECH CRUNCH (Nov. 15, 2015), http://techcrunch.com/2015/11/15/information-sharing-is-key-to-avoiding-a-cyberattack/.

[144] SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS 234 (2014).

[145] *Id.* at 235.

"blue hat" hackers[146] to identify vulnerabilities in existing software and creating a market niche of affordable cyber security tools for public consumption.

### *A. Private Sector Solutions to Cyber Security*

#### 1. Microsoft SDL and "Blue Hat" Hackers

After suffering a cyber attack in 2008,[147] Microsoft has become an industry leader in developing revolutionary cyber security software and strategies. In 2011, Microsoft launched the Security Development Lifecycle (SDL), a software development process that helps programmers build more secure software at lower costs.[148] Today, many companies use SDL to protect their own databases and, on average, Microsoft experts have found less vulnerability in newer products.[149]

In addition to utilizing internal resources to develop anti-terror software and sharing it with other firms, companies are enlisting the public's help to discover new solutions to cyber security. Microsoft provides financial incentives for "blue hat" hackers to devise new ways of protecting the company's data. For example, the Microsoft BlueHat Prize Contest offers $200,000 to competitors who design the most effective cyber security

---

146 *See infra* Part V.A.1.

147 Brian Ries, *Hackers' Most Destructive Attacks*, THE DAILY BEAST (Dec. 11, 2010), http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html (ranking an unknown hacker's use of the "Conficker" virus to infect various Microsoft operating systems as the sixth most infamous hack in the last twenty-five years).

148 *Security Development Lifecycle*, MICROSOFT (2015), https://www.microsoft.com/en-us/sdl.

149 *Id.*

solution.[150] The Google Vulnerability Reward Program awards up to $20,000 to each competitor who exposes a vulnerability in Google's operating system[151] and Firefox holds a similar contest.[152] By inviting ethical hackers to identify loopholes in existing software, the private sector can discover a panoply of promising techniques to better protect customer and employee privacy.

2. Securing Infrastructure Triggers Norm Cascades and Achieves Competitive Edge

An increasing number of companies are fortifying their infrastructure and setting new normative standards for cyber security. The cyber security insurance market has grown from a $100 million industry in 2003 to a $750 million industry in 2011 with the percentage of insured companies increasing from 25% in 2004 to 34% in 2008.[153] In 2009, 85% of firms had created the position of Chief Information Security Officer (CISO) compared to just 43% in 2006.[154] A CISO's duties include protecting data privacy, overseeing the company's security infrastructure and conducting digital forensic investigations.[155]

Additionally, companies are adopting preventative measures. For example, Facebook's wall of scalps is a virtual scrapbook of spammers, child

---

150 SHACKELFORD, *supra* note 23, at 219.

151 *Google Vulnerability Reward Program (VRP) Rules*, GOOGLE APPLICATION SECURITY (2016), https://www.google.com/about/appsecurity/reward-program/.

152 SHACKELFORD, *supra* note 23, at 219.

153 *Id.* at 249.

154 *Id.* at 227.

155 Margaret Rouse, *CISO (Chief Information Security Officer)*, TECHTARGET (Dec. 2013), http://searchsecurity.techtarget.com/definition/CISO-chief-information-security-officer.

predators, fraudsters and other criminals flagged by the company who attempted to breach a Facebook user's privacy.[156] This innovative and effective method of protecting Facebook users from cyber attacks has the potential to trigger a "norm cascade" throughout social media so Twitter, Instagram and Snapchat users can enjoy enhanced privacy as well.[157] Of course, investing in cyber security to maximize consumer privacy not only protects users but also helps private companies gain a valuable edge over less scrupulous competitors unwilling to consider privacy a priority.

### *B. The Government's Role in Preventing Cyber Terror*

Although the free market has plenty of power to combat cyber terror through competition and innovation, both the federal and state governments can maximize this potential through limited regulation. For example, the state can further incentivize the private sector's efforts in enhancing cyber security by mandating publicly disclosed ratings and awarding tax breaks to the companies that rank highest for developing a robust resistance to cyber attacks while permitting lawsuits against lower ranked companies that fail to adequately protect customer data.[158]

The Gramm-Leach-Bliley Act requires certain financial firms to inform customers of their information sharing policies and protect against the

---

[156] Elinor Mills, *At Facebook, Defense is Offense*, CNET (Jan. 31, 2011, 10:55 PM), http://www.cnet.com/news/at-facebook-defense-is-offense.
[157] SHACKELFORD, *supra* note 23, at 259.
[158] *Id.* at 235.

unauthorized access of customer records.[159] However, companies do not have a duty to disclose a security breach unless the Securities Exchange Commission (SEC) or state law mandates otherwise.[160] Forty-six states have passed such mandates, but some do not require disclosure if the appropriated information was not used to harm customers.[161]

This no-harm exception is misguided because the mere appropriation of sensitive information compromises privacy and discourages customers from communicating online. Of course, one could argue that ignorance is bliss, but legislation that mandates candor with customers when private data is breached provides valuable peace of mind and eliminates the powerful chilling effect caused by suspicion that data might have been breached in the past or may be breached in the future without means of confirmation. Still, legislation can play a major role in bolstering private sector security and exposing those who leave customer data vulnerable to public scrutiny.

In addition to using legislation, various states have attempted to improve cyber security in the private sector through litigation. In some states, individuals whose data was breached can sue the company holding that data for failing to use reasonable care in protecting it.[162] However, one of the major obstacles to judicial relief includes click-wrap agreements containing a clear

---

159 SHACKELFORD, *supra* note 23, at 238.
160 *Id.*
161 *Id.* at 239.
162 *Id.* at 242.

disclaimer that a company's security system is flawed and no reasonable consumer can rely on it.

Sony used a standard click-wrap agreement to dodge liability from the PlayStation Network hack in 2011[163] that leaked the names, addresses, birthdates, passwords and other personal information of approximately seventy-seven million users.[164] Still, some courts have sustained claims of negligence despite such agreements when there are latent vulnerabilities.[165] Although the case law in this area varies from state to state, the notion of holding companies to a duty of care and providing customers legal redress for a privacy breach encourages the private sector to diligently protect data or risk potential legal liability.

### *C. Employing Encryption to Protect Data*

Many cyber security experts consider encryption a powerful tool to protect sensitive data from unauthorized breach.[166] A quick Internet query of

---

[163] *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 968 (S.D. Cal. 2012) (citing exculpatory language: "There is no such thing as perfect security. . . we cannot ensure or warrant the security of any information transmitted to us through the PlayStation Network. . .").

[164] Benn Quinn & Charles Arthur, *PlayStation Network Hackers Access Data of 77 Million Users*, THE GUARDIAN (Apr. 26, 2011), http://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data.

[165] SHACKELFORD, *supra* note 23, at 243.

[166] Brian Behlendorf, Jane Fountain, Derek Khanna, Cindy Cohn & David Atkins, *Why Encryption is the Answer for Both Individual and National Security*, REINVENT (Mar. 14, 2016), http://reinvent.net/why-encryption-is-the-answer-for-both-individual-and-national-security/; Steve Pate, *Encryption as an Enabler: The Top 10 Benefits*, NETWORK WORLD (Apr. 26, 2013, 3:54 PM) http://www.networkworld.com/article/2165740/tech-primers/encryption-as-an-enabler—the-top-10-benefits.html; John Girard, *Realise the Full Benefits by Encrypting Hard Drive and Storage Media*, COMPUTER WEEKLY (Feb. 2009), http://www.computerweekly.com/feature/Realise-the-full-benefits-by-encrypting-hard-drive-and-storage-media.

ways to encrypt data reveals countless instructional websites people without a technical background can comprehend.[167] Moreover, encryption can be used on any level from securing vacation photos on a family's desktop to protecting a multinational corporation's confidential records. But despite its ease and relatively low cost, many companies have failed to encrypt customer data at the expense of privacy.

For example, Concentra, one of the nation's largest health care providers, compromised nearly 150 medical records after a thief stole an unencrypted company laptop from an employee's car in 2012.[168] Coca Cola made the same mistake in 2013 but on a grander scale when a disgruntled employee stole fifty-five unencrypted laptops from the company's Atlanta offices over a period of six years exposing approximately 74,000 records containing the names, addresses, social security numbers, salaries, and driver's license numbers of current and former employees.[169]

California law requires timely disclosure to any California resident whose unencrypted personal information is compromised, and both state and federal government agencies can levy fines against negligent companies for

---

[167] *See* Alex Castle, *How to Encrypt (Almost) Anything*, PCWORLD (Jan. 18, 2013, 3:36 PM), http://www.pcworld.com/article/2025462/how-to-encrypt-almost-anything.html; Whitson Gordon, *A Beginner's Guide to Encryption: What It Is and How to Set It Up*, LIFEHACKER (Jan. 27, 2014, 4:01 PM), http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946; Marc Lowe, *How to Encrypt Your Computer*, UCSF (Feb. 26, 2016, 5:10 PM), https://it.ucsf.edu/encrypt.

[168] Joseph Conn, *Unencrypted-laptop Thefts at Center of Recent HIPAA Settlements*, MODERN HEALTHCARE (Apr. 26, 2014, 10:02 AM), http://www.modernhealthcare.com/article/20140426/MAGAZINE/304269948.

[169] Mike Esterl, *Coca Cola: Stolen Laptops Had Personal Information of 74,000*, WALL ST. J. (Jan. 28, 2014, 9:37 PM), http://www.wsj.com/news/articles/SB10001424052702304632204579341022959922200.

failing to encrypt data.[170] Although these measures can encourage companies to take greater care securing electronic records in the future, once the data is released, the damage is done. For instance, stolen information can be instantly distributed to countless identity thieves making it nearly impossible to retrieve. Therefore, it is imperative companies of all sizes proactively invest in encryption to protect consumer privacy and avoid debilitating legal liability.

### *D. Affordable Tools and Techniques to Protect Individual Privacy*

On an individual level, protecting one's data and communication online is vital to restoring privacy and free speech on virtual platforms. The private sector has created numerous tools to achieve safety and secrecy when using technology. The HyperText Transfer Protocol Secure (HTTPS) is an easy way to encrypt communication with most major websites and is compatible with Firefox, Google Chrome and other popular search engines.[171] HTTPS can also protect communication to other Internet users via email and messenger if conducted through a web-based interface like Gmail or Yahoo.[172]

Additionally, the virtual private network (VPN) is an affordable and legal web proxy that masks a user's location when searching the Internet and allows for more secure communications when downloading and uploading

---

[170] Stephen Cobb, *Encryption Essential for Cyber Security: A Million Reasons to Encrypt Sensitive Data*, ESET (June 10, 2014, 9:15 AM), http://www.welivesecurity.com/2014/06/10/encryption-essential-for-cyber-security.

[171] Jennifer Kyrnin, *HTTPS*, ABOUT TECH (2015), http://webdesign.about.com/od/http/g/bldefhttps.htm.

[172] *HTTPS*, WIKIPEDIA , https://en.wikipedia.org/wiki/HTTPS (last visited December 10, 2015).

content through the network.[173] Although a VPN cannot make online connections completely anonymous, it provides employees a secure way to access their company's intranet, protects wireless transactions and allows users in oppressed regions to circumvent geo-restrictions and censorship.[174]

To achieve anonymity online, the Tor Project is a free and legal option that directs Internet traffic through more than 7,000 relays to conceal a user's location and identity from anyone conducting network surveillance, including the government.[175] To encrypt telephone calls and texts, users can download the application Signal for free to an IOS or Android device.[176] These are just a few examples of various affordable, legal and user-friendly products anyone can employ to protect one's privacy without surrendering the invaluable conveniences of technology.

### *E. Preventing the Sony Hack*

The Sony hack was massive and planned months in advance, but experts claim it could have been mitigated if not prevented entirely if Sony equipped its servers with stronger safeguards.[177] Despite falling victim to multiple attacks through the years, including the unprecedented PlayStation

---

[173] *Virtual Private Network*, WIKIPEDIA, https://en.wikipedia.org/wiki/Virtual_private_network (last visited December 10, 2015).

[174] *Id.*

[175] *Tor*, WIKIPEDIA, https://en.wikipedia.org/wiki/Tor_(anonymity_network) (last visited December 10, 2015).

[176] Andy Greenberg, *Signal, the Snowden-Approved Crypto App, Comes to Android*, WIRED (Nov. 2, 2015, at 10:55 AM), http://www.wired.com/2015/11/signals-snowden-approved-phone-crypto-app-comes-to-android.

[177] John Gaudiosi, *Why Sony Didn't Learn from Its 2011 Hack*, FORTUNE (Dec. 24, 2014, 9:00 AM), http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack.

Network hack in 2011, which compromised the personal data of about seventy-seven million gamers, Sony failed to enact rudimentary security measures like stratifying its servers so access to one does not yield access to all, using stronger passwords, encrypting stored data and conducting security education training for all employees.[178] Unfortunately, Sony had ineffective communication between numerous divisions resulting in a vulnerable decentralized network.[179]

Despite the 2011 PlayStation Network hack and 2012 PlayStation 3 hack, Sony leads the gaming console market in sales as consumers seem quick to forgive the entertainment giant for its failure to safeguard their data.[180] As a result, there was little incentive for Sony to bolster its cyber security infrastructure. This time, however, the hackers targeted Sony employees of all pay grades whose emails remain fully searchable on WikiLeaks and other online sources.[181] Given the great deal of embarrassment experienced from this exposure, perhaps Sony will finally make a serious investment to secure its servers even if its primary goal is to protect itself rather than consumers.

## VI. CONCLUSION

Most of the media's coverage of the Sony hack dealt with scandalous mudslinging between media moguls and Hollywood legends. But as the dust settled and the tabloids eyed the next hot scoop, the actual damage of the hack

---

178 *Id.*
179 *Id.*
180 *Id.*
181 *Sony Archives*, WIKILEAKS (Apr. 16, 2015), https://wikileaks.org/sony/press.

unfolded to be far more than an embarrassing flesh wound. Rather, the hack cut to the heart of the entertainment industry prompting censorship and chilling communication for fear of surreptitious surveillance and subsequent retaliation. It persuaded one of the world's largest and most accomplished media companies to not only edit its own picture because of unsubstantiated threats of physical force but also consider pulling it entirely before free speech-minded members of the public impassioned Sony to reinstate the premiere. The hack tops a growing list of cyber crimes that have caused hundreds of writers at the PEN American Center to triple check electronic communication and avoid topics of research for fear of reprisal.

Moreover, an increasing number of Americans nationwide are concerned for their privacy when using technology and will likely tailor their communication to conform to societal expectations of conventional and politically correct speech. Given that most communication among young adults is digital,[182] it is unsurprising that younger generations are more concerned than other age groups over the privacy of electronic devices. As a result, the First Amendment's protection of free speech may be academically revered but practically abandoned in the coming decades.

Fortunately, this prophecy need not come true. Groundbreaking private sector innovation along with effective government regulation can successfully

---

[182] Frank Newport, *The New Era of Communication Among Americans*, GALLUP (Nov. 10, 2014, 4:25 PM), http://www.gallup.com/poll/179288/new-era-communication-americans.aspx (citing survey that shows texting is the dominant way of communication for Americans under 50).

combat cyber terror and restore a sense of security in technology. Microsoft's SDL strategy for cyber security has helped hundreds of companies protect customer data and Facebook's wall of scalps has successfully squashed cyber terror at its source while setting a powerful standard for other social media sites harboring millions of young Americans' posts, photos and messages. Moreover, government regulation requiring companies to alert customers to data breaches and legislation providing judicial relief against companies that fail to adequately protect data incentivizes the private sector to prioritize cyber security or risk public scrutiny and legal liability. Finally, individuals can recapture their privacy by employing free and user-friendly software like Signal to encrypt text messages, virtual private networks to guard communication with websites and the Tor Project to achieve online anonymity.

Strengthening cyber security is crucial to not only protect the entertainment industry and private sector from malicious hackers but also safeguard the American people's sensitive data and electronically stored communication. Only when Americans feel secure using technology will the blessings of the First Amendment be fully realized.