1-1-2015

How Sony Can Impact Your Privacy

Nicole Fukuoka

HOW SONY CAN IMPACT YOUR PRIVACY

Cyber security is not just an issue for celebrities with scandalous selfies stored in their iClouds. On average, it takes companies thirty-two days and more than $1 million dollars to resolve a single, successful cyber attack.[1] The most recent privacy invasion on Sony Pictures shook more than just loose change from its victim's pockets—it rattled the nation.[2] The highly publicized hack exposed corporations' vulnerabilities to the attacks of anonymous enemies that operate in the lawless battleground of cyberspace. More importantly, Sony's response to the incident highlighted the lack of cyber security legislation needed to prevent businesses from enduring similar incidents.[3]

Sony's CEO claimed that the financial losses from the hack were not substantial enough to disrupt the well being of the company.[4] However, the attack revealed that cyber breaches can cost companies much more than money. Not only were Sony's executives nationally humiliated by offensive remarks that were leaked from their confidential emails, but they also may lose bargaining power and the industry's trust for future business deals.[5] Even more unnerving than the company's expansive losses, was the realization that American corporations are not prepared for the warriors of the web.[6] After decades of failed attempts to enact legislation to protect the nation from these kinds of devastating incidents, lawmakers are finally making cyber security a top priority.[7]

---

[1] Ponemon Institute, *2013 Cost of Cyber Crime Study: United States*, PONEMON INST. RESEARCH REPORT, (Oct. 2013), *available at* http://media.scmagazine.com/ documents/54/ 2013_us_ccc_report_final_6-1_13455.pdf.

[2] The Associated Press, *Sony Pictures CEO: Call to Google Got 'The Interview' Out*, THE NEW YORK TIMES (Jan. 9, 2015, 1:42 AM), http://www.nytimes.com/aponline/2015/01/08/us/ap-us-sony-hack-ceo-interview.html

[3] Jose DelReal, *Eyes Turn to the Next Congress as Sony Hack Exposes Cybersecurity Flaws*, THE WASHINGTON POST (Dec. 18, 2014), http://www.washingtonpost.com/blogs/ post-politics/wp/2014/12/18/eyes-turn-to-the-next-congress-as-sony-hack-exposes-cybersecurity-flaws/.

[4] The Associated Press, *supra* note 2.

[5] Susanna Kim, *How the Hacked Information From Sony Could Affect its Business*, ABCNEWS (Dec. 11, 2014), http://abcnews.go.com/Business/hacked-information-sony-affect-business/story?id=27533807.

[6] DelReal, *supra* note 3.

[7] Charles Blanchard, *Congress Ratchets Up Cyber Incident Reporting and Supply Chain Security Requirements*, ARNOLD & PORTER LLP (Jan. 7, 2015), http://www.arnoldporter .com/publications.cfm?action=advisory&u= CongressRatchetsUpCyberIncident ReportingandSupplyChainSecurityRequirements&id=1213&p=-1.

Two bills that are speculated to be reintroduced to congress this year, the Cyber Intelligence Sharing and Protection Act (CISPA)[8] and the Cybersecurity Information Sharing Act (CISA),[9] have controversial legislative histories. Both measures aim to give companies an offensive advantage to cyber threats, but come at the high cost of compromising their consumers' privacy.[10] This tradeoff begs the question of whether it is in society's best interest to reduce the risks of future cyber attacks from happening, or if increased cyber security is not worth the price of government agencies like the Department of Justice and the National Security Agency having more access to the public's private information.

To answer these questions, one must consider whether corporations should be more concerned about keeping classified materials from hackers, or protecting the privacy of their customers from the government. Despite mounting concerns that the government is pushing the public's privacy boundaries, the government is less of a threat than hackers, especially to businesses. While no one wants to live in a Big Brother society, keeping sensitive information out of the hands of those who may use it to steal from, control, or even physically harm the American people is a price worth paying.

Cyber Security Legislation in Question:

Two of the most prominent bills that have resurfaced following the Sony Hack, are the controversial measures CISPA and CISA.[11] On January 9, 2015, Representative Dutch Ruppersberger reintroduced CISPA to Congress. CISPA previously passed the House of Representatives twice, but was rejected by the Senate in 2012 and was then stalled by the Senate in 2013 over privacy concerns.[12] The objective of CISPA was to prevent cyber attacks by increasing voluntary information sharing between private companies and the government in the event of, or in suspicion of, a cyber attack.[13]

---

[8] Zack Whittaker, *Congress Revives CISPA, and it may get the White House's Support this Time*, ZDNET (Jan. 9, 2015), http://www.zdnet.com/article/after-sony-congress-revives-cispa-will-be-the-death-of-the-fourth-amendment/.

[9] DelReal, *supra* note 3.

[10] Whittaker, *supra* note 9.

[11] DelReal, *supra* note 3.

[12] *Id.*

[13] Taylor Wofford, *Meet the New CISPA, Same as the Old CISPA*, NEWSWEEK (Jan. 14, 2015), http://www. newsweek.com/meet-new-cispa-same-old-cispa-299375.

This year, Senator Dianne Feinstein is also expected to restart her stalled cyber legislation, CISA, which like CISPA, encourages information sharing between the private sector and the government to help protect businesses against cyber attacks.[14] Under CISA, businesses are immune from being sued for sharing individuals' private information with the government, if the information can be used to prevent a cyber threat.[15]

Both CISPA and CISA were highly contentious measures because opponents feared that they would not be efficient at preventing cyber attacks, and would violate the American people's Fourth Amendment rights by granting the government too much access to the public's confidential information.[16] However, Sen. Feinstein and Rep. Ruppersberger believe that the incident with Sony demonstrated how dire cyber security legislation is needed to get the government and private entities working together to stop the cyber enemy.[17]

Proponents of Cyber Security Legislation:

Proponents of cyber security legislation assert that the Sony hack revealed that America's enemies are no longer armed with just physical threats such as guns and explosives.[18] Instead, our adversaries are increasingly utilizing cyber weapons that can present an even greater threat to America's security interests.[19] Both Senator McCain and President Obama blame the administration's lack of effective cyber security legislation as a major contributing factor for what happened to Sony.[20] Proponents of CISPA and CISA believe that by increasing communication between government agencies and private corporations, the government will be able to prevent cyber attacks before they happen.[21]

Representative Jim Langevin, Co-chair of the House Cyber Security Caucus, stated that the new Congress should move quickly to pass "a comprehensive cyber security information sharing bill to allow the federal government to share what it knows about threats in cyberspace with the private

---

14 DelReal, *supra* note 3.

15 Gregory McNeal, *Controversial Cybersecurity Bill Known as CISA Advances out of Senate Committee*, FORBES (July 9, 2014), http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/.

16 *Id.*

17 DelReal, *supra* note 3.

18 *Id.*

19 *Id.*

20 *Id.*

21 McNeal, *supra* note 16.

sector, and vice versa" because he believes that what happened to Sony is a clear indication of the danger that exists to all corporations in cyberspace.[22] Sen. Feinstein stated that legislation like CISA will be a counterpunch to the countless cyber criminals who steal "personal information from retailers and trade secrets from innovative businesses" on a day-to-day basis.[23]

In addition to protecting confidential consumer information, the new cyber security legislation may be able to save corporations money.[24] In 2014, private corporations spent $4.1 billion dollars on cyber security, yet major financial institutions like JP Morgan and large corporations like Home Depot and Sony were still hacked.[25] Corporations are not alone in expending vast sums of money to protect their data. Since 2010, the government has invested $59 billion in data protection, but has still not been able to protect its agencies from hackers.[26] Due to the interdependence of private corporations and government entities in the realm of cyberspace, the former Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, Alan Raul, suggested that corporations stop wasting millions of dollars on ineffective cyber protections and start using government-operated network monitoring technology.[27]

"The big banks, big retailers and big media companies whose hacks make the front pages are not being penetrated because they've skimped on security out of sloth, stupidity or greed," said Raul.[28] He claimed that despite corporations' massive investments in cyber security, there was nothing more they could do to protect themselves from hackers than the government could. Instead, Raul suggests that corporations stop fighting this uphill battle alone, and let the government develop a program, like EINSTEIN, that can be used by businesses nationwide to protect confidential information. CISPA aims to enact a system like this.[29]

---

22 DelReal, *supra* note 3.

23 *Id.*

24 Ailya Sternstein, *Federal Cybersecurity Spending is Big Bucks. Why Doesn't it Stop Hackers?*, NEXTGOV (Jan. 8, 2015), http://www.nextgov.com/cybersecurity/2015/01/has-spending-nearly-60-billion-federal-cybersecurity-stopped-hackers/102534/.

25 *Id.*

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.*

Opponents of Cyber Security Legislation:

While most people agree that cyber security legislation needs to be enacted to better protect the American public and businesses from hackers, many have concerns with the proposed information sharing bills CISPA and CISA.[30] Opponents of the proposed legislation are fearful that government agencies like the NSA will use the laws to abuse the public's privacy rights.[31]

Both bills are drafted broad enough to allow companies to share people's confidential information with the government without warrants or other legal procedures if they suspect the information could be related to a cyber threat.[32] This information would include: emails, text messages, stored cloud files, and internet history searches.[33] Proponents of the bills argue that they are necessary to keep that exact same data away from foreign hackers and to halt cyber attacks before they happen.[34] However, opponents like Senators Ron Wyden and Mark Udall fear that the government will "exploit loopholes to collect Americans' private information in the name of security."[35] They also argue that cyber security legislation without "strong protections for Americans' constitutional privacy rights" will not only be ineffective, but it will also actually harm businesses.[36]

Why it Matters:

Even if CISA or CISPA do not mature into laws due to privacy concerns, cyber security legislation is coming. It is not only pertinent to keep corporations educated about potential new laws, but also to inform them about the importance of cyber protection. For example, breached trade secrets and intellectual property are not only sizeable financial losses, they can also lead to costly litigation because victims have standing to bring a class action suit against the business.[37] Additionally, information sharing between the

---

30 McNeal, *supra* note 16.

31 *Id.*

32 Chloe Albanesius, *What is CISPA, and Why Should You Care?,* PCMAG (April 22, 2014), http://www.pcmag.com/ article2/0,2817,2417993,00.asp.

33 *Id.*

34 *Id.*

35 McNeal, *supra* note 16.

36 *Id.*

37 Troutman Sanders, *5 Reasons Sony Pictures Will Be a Cybersecurity Inflection Point*, INFORMATION INTERSECTION (Dec. 19, 2014), http://www.informationintersection.com/2014/12/5-reasons-sony-pictures-will-be-a-cybersecurity-inflection-point/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

government and private sector is beneficial for businesses because companies do not have the robust resources needed to protect themselves from sophisticated privacy invasions, particularly those from foreign enemies.[38]

Therefore, from a business perspective, it is advantageous to sacrifice some of the public's privacy rights to the government in exchange for the ability to keep their confidential information out of the hands of hackers. While there is always the potential for government abuse of personal information, there is a much greater risk of that same information being used for more lecherous purposes by cyber criminals.

NICOLE FUKUOKA*

[38] *Id.*

* Editor-in-Chief Elect, *Emory Corporate Governance and Accountability Review*; J.D. Candidate, Emory University School of Law (2016); B.A., University of Southern California. I would like to thank Harrison Jones for his guidance during the early stages of this perspective, and Drew Case for his assistance during the drafting process that helped me develop this piece to its full potential.