Cybersecurity Reform in the Wake of the OPM Breach

"We already know many of the steps necessary to reduce the likelihood of a cyber 9/11, yet many of these actions have not yet been taken in either the government or in the private sector."[1]

I. INTRODUCTION

In 2015, the Office of Personnel Management's (OPM) computer systems suffered a series of devastating cyber attacks that uncovered roughly 21.5 million federal employees' personal information.[2] The breaches—attributed to Chinese hackers—resulted in the exposure of federal employees' extremely sensitive information, including Social Security numbers.[3] Over the past decade, similar cyber attacks on consumers' personal information have occurred within the private sector with alarming frequency.[4] The OPM

1. Jennifer Steinhauer, *Cybersecurity Bill Is Latest to Be Delayed in Senate*, N.Y. TIMES (Aug. 5, 2015), http://www.nytimes.com/2015/08/06/us/politics/cybersecurity-bill-is-latest-to-be-delayed-in-senate.html (quoting U.S. Senator Susan Collins).

2. *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html [http://perma.cc/6KTJ-ANV5] (describing vast and detrimental scope of OPM breach); *see also Cybersecurity Incidents: What Happened*, OPM.GOV, https://www.opm.gov/cybersecurity/cyber security-incidents (last visited Oct. 24, 2016) [http://perma.cc/HB86-WCDP] (identifying victims of breach).

3. *See* Davis, *supra* note 2. The compromised information also included federal employees' financial history, medical history, and addresses. *See id.* Some months after the breaches, OPM announced the theft of six million people's fingerprints as well. *See* Allison Grande, *OPM Fingerprint Hack Exposes Liabilities in Biometric Data*, LAW360 (Sept. 24, 2015), http://www.law360.com/articles/707030/opm-fingerprint-hack-exposes-liabilities-in-biometric-data [http://perma.cc/A5DV-CKCW].

4. *See* Thad A. Davis et al., *The Data Security Governance Conundrum: Practical Solutions and Best Practices for the Boardroom and the C-Suite*, 2015 COLUM. BUS. L. REV. 613, 615 (2015) (noting explosion of recent data security breaches and resulting boardroom pressure from regulators and plaintiffs). During the holiday shopping rush in 2013, hackers lifted credit card information from forty million Target customers. *See* Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 17, 2014), http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data [http://perma.cc/CY9V-FGJ7]. In 2014, hackers stole over fifty million customer credit card numbers and email addresses from Home Depot. *See* Shelly Banjo, *Home Depot Hackers Exposed 53 Million Email Addresses*, WALL STREET J. (Nov. 6, 2014), http://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282. That same year, hackers gained access to nearly eighty million bank accounts belonging to both individuals and small businesses. *See* Jessica Silver-Greenberg et al., *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES: DEALBOOK (Oct. 2, 2014), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues [http://perma.cc/TLH8-BDQD]. In 2015, Anthem, a major health insurer, disclosed that hackers stole the personal information of almost eighty million customers and employees, specifically their "names, birthdays and Social

breaches highlight a disturbing trend concerning the federal government's ill-preparedness in dealing with cybersecurity incidents in the public sector.[5]

An OPM computer systems audit occurring prior to the OPM breach unveiled alarming security failings.[6] The audit exposed OPM's decentralized information security, and that many employees tasked with managing the information security system were not information technology professionals.[7] Many systems were operating without valid authorization, including two support systems that placed over sixty-five percent of OPM's systems at risk.[8] OPM's knowledge of these cybersecurity deficiencies over a period of several years demonstrates that the federal government should make changes to its information security initiatives.[9]

Cybersecurity is a dynamic and highly technical field, and the government has historically been reluctant to wade into the fray.[10] Presently, a hodgepodge

Security numbers." *See* Anna Wilde Mathews, *Anthem: Hacked Database Included 78.8 Million People*, WALL STREET J. (Feb. 24, 2015), http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.

5. *Compare* Mathews, *supra* note 4 (exemplifying private sector cybersecurity failure through Anthem security breach), *with* Davis, *supra* note 2 (describing government cybersecurity breach under Obama Administration), *and* Dan Friedman, *Hackers Hit IRS, Gain Access to Information on 100,000 Taxpayers*, N.Y. DAILY NEWS (May 27, 2015), http://www.nydailynews.com/news/national/hackers-hit-irs-gain-access-info-100-000-taxpayers-article-1.2236738 (presenting additional governmental IRS breaches).

6. *See* U.S. OFFICE OF PERS. MGMT., OFFICE OF THE INSPECTOR GEN. OFFICE OF AUDITS, FINAL AUDIT REPORT: FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT 5 (2014), https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf [http://perma.cc/ZY5Z-3QCL] [hereinafter FINAL AUDIT REPORT 2014] (recounting years of OPM's informational security weaknesses); Derek Major, *After the OPM Breach: Ripple Effects and Lingering Questions*, GCN (Sept. 18, 2015), https://gcn.com/articles/2015/09/18/opm-hack-military-ripple-effect.aspx [http://perma.cc/SPK4-VBKK] (revealing OPM breach resulted from stolen vendor credentials).

7. *See* FINAL AUDIT REPORT 2014, *supra* note 6, at 5 (explaining employees must manage information security in addition to other duties); Joe Davidson, *Following the OPM Data Breach, Uncle Sam Needs to Step Up Recruitment of Cyber Talent*, WASH. POST (Aug. 17, 2015), http://www.washingtonpost.com/news/federal-eye/wp/2015/08/16/following-the-opm-data-breach-uncle-sam-needs-to-step-up-recruitment-of-young-cyber-talent/ [http://perma.cc/RL27-ULJ2] (advocating for improving recruitment of cyber talent).

8. *See* FINAL AUDIT REPORT 2014, *supra* note 6, at 10 (describing various systems OPM breach affected). The audit also revealed that OPM's Federal Investigative Services, which facilitate background and security clearance checks, was also operating without a valid authorization. *See id.* In addition, the OPM data was not encrypted despite its extremely sensitive nature. *See* Aaron Boyd, *OPM Breach a Failure on Encryption, Detection*, FED. TIMES (June 19, 2015), http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/ [http://perma.cc/NN26-MDYC].

9. *See* David Auerbach, *The OPM Breach Is a Catastrophe*, SLATE (June 16, 2015), http://www.slate.com/articles/technology/future_tense/2015/06/opm_hack_it_s_a_catastrophe_here_s_how_the_government_can_stop_the_next.html [https://perma.cc/4NPV-8Q32] (identifying long-standing and embarrassing security failures in initial audit); Eric Yoder, *OPM Response to Cyberbreach Challenged Again*, WASH. POST (Sept. 14, 2015), http://www.washingtonpost.com/news/federal-eye/wp/2015/09/14/opm-response-to-cyberbreach-challenged-again/ [http://perma.cc/R7XZ-XAS6] (describing OPM system audit and continued dysfunction).

10. *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1510 (2013) (identifying government's purported lack of ability to regulate cybersecurity); Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 232 (2013) (acknowledging absence of federally mandated private sector cybersecurity standards).

of laws, regulations, and an executive order govern how the federal government protects its information.[11] These varied and confusing standards also provide little recourse for the victims of cyber breaches seeking damages through civil suits.[12] While Congress has proposed legislation to address the issue of cybersecurity, inexplicably, this legislation often focuses heavily on *responding* to cyber attacks rather than *preventing* them.[13]

This Note will confront the question of whether the Cybersecurity Act of 2015[14] (Cybersecurity Act)—stemming from the proposed Cybersecurity Information Sharing Act[15] (CISA) and Federal Cybersecurity Enhancement Act of 2015[16] (FCEA) (collectively referred to as S.754)—can adequately address the security and civil liability inadequacies that exist under the current legislative framework.[17] Part II.A will explore the existing patchwork of statutes, executive orders, and administrative entities that currently control state protection of personal information and state responses to cyber attacks.[18] Part II.B will examine civil liability issues in both the private and public sectors under the current legislative framework.[19] Part II.C will detail the provisions of S.754 and the Cybersecurity Act.[20] Following an analysis of the Cybersecurity Act's strengths and weaknesses, Part III of this Note will provide proposed changes particularly in the areas of cyber attack protection and liability concerns.[21] Ultimately this Note argues that the Cybersecurity Act is inadequate to address the issues of protection and redress that currently exist.[22]

11. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739-40 (Feb. 12, 2013) (establishing cybersecurity information sharing framework); Davis et al., *supra* note 4, at 629 (identifying absence of "united regulatory front on . . . data security"); Dana Rosenfeld & Donnelly McDowell, *Moving Target: Protecting Against Data Breaches Now and down the Road*, 28 ANTITRUST 90, 90 (2014), http://www.kelleydrye.com /publications/articles/1859/_res/id=Files/index=0/Summer14-RosenfeldC.pdf [https://perma.cc/KP2D-TBGG] (noting absence of single legal data security standard).

12. *See* Aliya Sternstein, *Why the Lawsuit Against OPM over the Massive Data Breach Faces an Uphill Battle*, NEXTGOV (July 1, 2015), http://www.nextgov.com/cybersecurity/2015/07/why-lawsuit-against-opm-over-massive-data-breach-faces-uphill-battle/116701 [http://perma.cc/QBT4-YXST] (articulating difficulties cyber-breach victims face proving damages).

13. *See* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. § 103 (2015) (discussing procedures to share "cyber threat indicators," demonstrating lack of preventative measures).

14. Cybersecurity Act of 2015, Pub. L. No. 114-113, 129 Stat. 2242 (2015).

15. S. 754 §§ 101-110 (representing CISA portion of S. 754).

16. S. 754 §§ 201-209 (representing FCEA portion of S. 754). This Note collectively refers to CISA and FCEA in textual sentences as S.754.

17. *See infra* Part III.

18. *See infra* Part II.A; *see also* Rosenfeld & McDowell, *supra* note 11, at 90 (reiterating multiple regulations apply to data security).

19. *See infra* Part II.B.

20. *See infra* Part II.C.

21. *See infra* Part III.

22. *See infra* Part IV (concluding further steps necessary); *see also* Jay P. Kesan & Carol M. Hayes, *Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals*, 2014 MICH. ST. L. REV. 1475, 1530-31 (2014) (discussing previous bill's similar inadequate civil liability framework); Sales, *supra* note 10, at 1545 (suggesting legislative solution must "harden[] vulnerable targets"); Elias Groll, *A*

II. HISTORY

A. Existing Cybersecurity Legislation and Regulation

The Federal Information Security Management Act of 2002[23] (FISMA) gives the Director of the Office of Management and Budget (OMB) the power to issue security standards for federal systems.[24] These standards are based on mandatory minimum requirements designed by the National Institute of Standards and Technology (NIST).[25] The standards issued are mandatory for all federal systems, although the head of a federal agency may elect to implement more rigorous standards than those the NIST recommends.[26] Commentators critique FISMA as an ineffective tool to ensure information security within the federal government.[27]

In 2014, Congress amended FISMA to provide a more comprehensive legislative framework for federal information security.[28] The amended FISMA leaves the power to oversee the federal information security scheme with the Director of OMB, but indicates that the Director must work in conjunction with the Secretary of Homeland Security.[29] The amended FISMA also details the

Cybersecurity Bill Light on Security, Heavy on Corporate Protection, FOREIGN POL'Y (Sept. 15, 2015), http://foreignpolicy.com/2015/09/14/a-cybersecurity-bill-light-on-security-heavy-on-corporate-protection/ [http://perma.cc/EU69-AQTJ] (suggesting S.754 inadequate to improve security measures).

23. 40 U.S.C. § 11331 (2012).

24. *See id.* § 11331(b)(1)(A) (designating OMB's role of "promulgat[ing] information security standards").

25. *See id.* § 11331(b)(1). The NIST categorizes information based on risk levels. *See* 15 U.S.C. § 278g-3(b)(1)(A) (2012) (outlining requirements for standards issued). The NIST also establishes minimum security requirements for each category of information, as well as guidelines for how to address and respond to security breaches. *See id.* § 278g-3(b)(1)(C) (describing content of issued standards). In creating the information security standards, the NIST consults with several other federal agencies. *See id.* § 278g-3(c)(1) (listing examples of cooperating agencies).

26. *See* 40 U.S.C § 11331(c) (outlining potential alternative methods for issuing information standards). The alternative method implemented by the head of the agency must be cost-effective. *See id.*

27. *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 45 (2013) (detailing several critiques of FISMA); Brian B. Kelly, Note, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. REV. 1663, 1684 (2012) (noting criticism concerning FISMA's oversight of cybersecurity). Problematic issues include:

> [I]nadequate resources, a focus on procedure and reporting rather than operational security, lack of widely accepted cybersecurity metrics, variations in agency interpretation of the mandates in the act, excessive focus on individual information systems as opposed to the agency's overall information architecture, and insufficient means to enforce compliance both within and across agencies.

FISCHER, *supra*, at 45.

28. *See* Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551(1) (Supp. II 2014) (describing purpose of amendment).

29. *See id.* § 3553(a)-(b) (describing roles for OMB and Homeland Security); *Federal Information Security Modernization Act (FISMA)*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/fisma (last visited Oct. 25, 2016) [http://perma.cc/RYD8-UJMU] (clarifying OMB holds "oversight authority").

responsibilities assigned to the heads of federal agencies to prevent information security breaches.[30] Additionally, it establishes extensive reporting requirements for federal agencies in the information security realm.[31] To further enhance cybersecurity measures, the amended FISMA established a federal information security incident center to coordinate and assist information security efforts.[32]

On February 12, 2013, President Obama signed an executive order titled "Improving Critical Infrastructure Cybersecurity" (EO).[33] To achieve its stated purpose, the EO allows the federal government to convey information about cyber threats to targeted private organizations in order to protect critical infrastructure.[34] The EO also creates the Cybersecurity Framework—a set of voluntary security standards to provide cybersecurity guidance.[35]

The National Cybersecurity Protection Act of 2014 (The Act)[36] created the National Cybersecurity and Communications Integration Center (NCCIC).[37] The NCCIC's objective is to coordinate information shared about cybersecurity risks between federal and private entities, and to act as an informational resource.[38] The Act mandates federal agencies to coordinate and implement

30. *See id.* § 3554(a)(1)(b) (requiring agency heads to create compliant information security programs). In addition to maintaining information security systems for their respective agencies, agency heads are required to subject those systems to periodic testing to ensure their efficacy. *See id.* § 3554(a)(2)(D) (describing responsibility of agency heads to ensure secure systems). Agency heads are also directed to establish a Chief Information Officer (CIO) whose "primary duty" is information security and who "possesses professional qualifications." *See id.* § 3554(a)(3)(A).

31. *See id.* § 3554(b)(7) (requiring federal agencies to have "procedures for detecting, reporting, and responding to security incidents"). Each federal agency is further responsible for issuing an annual report to multiple other agencies and federal committees that details the information security issues that arose and procedures that were used in the past year. *See id.* § 3554(c)(1)(A) (explaining which agencies should receive report). In turn, the OMB Director is required to submit an annual report to Congress concerning the efficacy of information procedures utilized government wide. *See id.* § 3553(c) (describing mandated report).

32. *See id.* § 3556 (describing responsibilities of federal information security incident center).

33. *See generally* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013) (outlining approach to protect critical infrastructure). "[C]ritical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." *Id.* at 11,739.

34. *See id.* at 11,739-40 (outlining procedure for sharing threat information with private entities). Some critics imply that a two-way exchange of information between public and private sectors would be more effective than the one-way flow of information between sectors that the EO established. *See* Kesan & Hayes, *supra* note 22, at 1515-16 (explaining one-way information flow weakness).

35. *See* Exec. Order No. 13,636, 78 Fed. Reg. at 11,741 (explaining Cybersecurity Framework). Experts criticize the voluntary nature of the Cybersecurity Framework as ineffective when compared to a program requiring mandatory compliance. *See* Kesan & Hayes, *supra* note 22, at 1545 (considering "inconsistent implementation" an emblematic problem for voluntary programs).

36. 6 U.S.C. § 148 (Supp. II 2014).

37. *See id.* § 148(b) (establishing NCCIC within Department of Homeland Security).

38. *See id.* § 148(c)(3), (5) (describing NCCIC function and outlining NCICC's risk analysis of cybersecurity incidents). If requested, the NCCIC may provide aid, advice, or response assistance to any entity. *See id.* § 148(c)(6)-(7).

critical infrastructure attack response plans.[39]

B. Civil Liability Under the Current Framework

1. Standing

Under the current legislative and regulatory framework for information security, civil suits against the federal government for breaches or violations of privacy often raise standing issues.[40] In *Clapper v. Amnesty International USA*,[41] the plaintiffs hoped to establish injury in fact, and therefore standing, on the theory that the necessary measures to protect their confidential communications from government surveillance placed a procedural and financial burden upon them.[42] The Court held that this harm was self-inflicted and not the result of impending external harm, and therefore decided that the plaintiffs had no standing.[43]

Clapper set the stage for standing issues surrounding information security breaches.[44] Like in *Clapper*, security breaches often result in exposure to possible future harms that have not come to fruition at the time of litigation: In the OPM case, the potential future harm at stake is identity theft stemming from stolen personal information.[45] Cyber-breach victims are first faced with the difficult task of demonstrating a harm that has not yet occurred, and then later proving any harm they do incur resulted from that specific breach.[46]

39. *See id.* § 149 (describing numerous entities involved in formulating critical infrastructure response plans).

40. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) (holding no standing due to lack of injury in fact). To establish standing, a plaintiff must demonstrate injury in fact, that is "concrete and particularized . . . and . . . 'actual or imminent, not "conjectural" or "hypothetical."'" Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (citations omitted).

41. 133 S. Ct. 1138 (2013).

42. *See id*. at 1150-51 (explaining plaintiffs' theory of injury in fact). Plaintiffs advanced their theory in the context of a recently enacted statute that permitted surveillance of foreign targets. *See id.* at 1144.

43. *See id.* at 1151 (articulating Court's rejection of Second Circuit precedent). The Court explained that permitting the establishment of standing through self-inflicted harm would result in a lower standing standard. *See id.*

44. *See* Alison Frankel, *The 7th Circuit Just Made It a Lot Easier to Sue Over Data Breaches*, REUTERS BLOG (July 21, 2015), http://blogs.reuters.com/alison-frankel/2015/07/21/the-7th-circuit-just-made-it-a-lot-easier-to-sue-over-data-breaches/ [http://perma.cc/BZG4-8KU3] (considering *Clapper* standing standard in class action suits for data breaches).

45. *See* Alison Frankel, *Suits Pile Up After U.S. Reveals Data Breach Affected Millions*, REUTERS BLOG (Aug. 17, 2015), http://blogs.reuters.com/alison-frankel/2015/08/17/suits-pile-up-after-u-s-reveals-data-breach-affected-millions/ [http://perma.cc/5LF2-2GHL] (discussing difficulty of recovering without demonstrable concrete injury). The Seventh Circuit recently held that a future injury caused by a data breach could be sufficient to satisfy standing inquiries, so long as there is a "substantial risk" of the harm actually occurring. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (recognizing some future harms constitute standing). However, other jurisdictions may interpret the level of risk incurred by data-breach victims more narrowly because no OPM-related suit was brought in the Seventh Circuit. *See* Frankel, *supra*.

46. *See* Matthew A. S. Esworthy & Aaron M. Danzig, *Will the Court Define "Actual Damages" in the OPM Cyber-Attack Lawsuit?*, A.B.A. (Sept. 17, 2015), http://apps.americanbar.org/litigation/committees

Courts have varying interpretations of what constitutes injury in fact in data breach cases.[47] A recent Supreme Court case clarified that even statutory causes of action require demonstrations of actual harm.[48] Some courts find that when actual identity theft or fraudulent charges result from a data breach, injury in fact is satisfied.[49] Courts disagree, however, on whether increased risk of identity theft alone can satisfy the injury in fact requirement.[50]

In response to the OPM data hack, a class action suit was filed in the D.C. Circuit Court of Appeals alleging violations of the Privacy Act of 1974.[51] The Privacy Act requires that the federal government protect records to ensure confidentiality of information, "which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[52] Notably, the Privacy Act goes beyond a simple showing of standing and requires demonstration of actual monetary damages in order to recover.[53] Several commentators anticipate difficulty in demonstrating

/criminal/articles/fall2015-0915-will-court-define-actual-damages-opm-cyber-attack-lawsuit.html [http://perma.cc/7WMH-XHEK] (discussing issue of proving evidential links between data breach to adverse consequences).

47. *See supra* notes 40, 45 (considering different injury in fact interpretations critical to standing argument).

48. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549-50 (2016). The Court clarified that when a purely procedural violation of a statute results in no harm, injury in fact cannot be satisfied. *See id.* at 1550. The Court acknowledged, however, that intangible harms can still constitute injury in fact in some cases. *See id.* at 1549.

49. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (basing standing on fraudulent charges); *Remijas*, 794 F.3d at 692 (noting 9,200 customers fraudulently charged resulted in harm); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding standing based on fraudulent charges, restricted access to bank accounts, and fees).

50. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011) (holding hypothetical injuries insufficient for standing), *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958-59 (D. Nev. 2015) (finding increased risk insufficient to confer standing), *and* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654 (S.D. Ohio 2014) (finding increased risk insufficient absent "certainly impending" harm), *with In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014) (finding risk of potential harm and mitigation costs sufficiently establishing standing), *and In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962-63 (S.D. Cal. 2014) (identifying risk of harm sufficient for standing purposes).

51. *See* 5 U.S.C. § 522a (2012) (codifying Privacy Act); Class Action Complaint, Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., No. 1:15-cv-1015 (D.D.C., June 29, 2015), 2015 WL 4039005 (representing class action lawsuit); *see also* Aliya Sternstein, *Federal Employee Union Sues over OPM Hack, Citing Financial and Emotional Distress*, NEXTGOV (June 29, 2015), http://www.nextgov.com/cybersecurity/2015/06/federal-employee-union-sues-hacked-opm-over-financial-and-emotional-distress/116563/ [http://perma.cc/N5ER-4X76] (describing lawsuit and clarifying plaintiffs' suits based on financial and emotional distress).

52. 5 U.S.C. § 522a(e)(10) (describing privacy breach cause of action); *see also* Robert Barnes, *Justices Weigh Whether Privacy Act Violations Allow for Distress Damages*, WASH. POST (Nov. 30, 2011), https://www.washingtonpost.com/politics/justices-weigh-whether-privacy-act-violations-allow-for-distress-damages/2011/11/30/gIQA91cMEO_story.html [http://perma.cc/3PHZ-99CU] (describing case alleging Privacy Act breach by revealing HIV diagnosis).

53. *See* Fed. Aviation Admin. v. Cooper, 132 S. Ct. 1441, 1455-56 (2012) (holding actual damages necessary to recover under Privacy Act). Justice Alito specifically explained that emotional and mental distress do not qualify as actual damages under the Privacy Act, and that plaintiffs must also demonstrate that privacy infringements also caused monetary harm. *See id.* at 1455.

monetary damages to establish injury in fact in the OPM case.[54] Whether injury in fact exists depends largely on whether a court takes a narrow or broad view of injury in fact, and if the broader view prevails, the scope of liability in the suit is potentially massive considering the millions of people impacted by the breach.[55]

2. Confusing Standards

Civil liability for cyber attacks is often complicated by the numerous government agencies that may claim purview over the matter, as well as uncertainty surrounding which standards must be adhered to in order to prevent liability.[56] This ambiguity played out in *FTC v. Wyndham Worldwide Corp*.,[57] in which the FTC brought an enforcement action against Wyndham for failure to prevent cyber breaches of consumer information due to practices that the FTC argued constituted unfair and deceptive business practices.[58] On interlocutory appeal, the Third Circuit ruled for the first time that the FTC possessed the authority to enforce private companies' data security through the Federal Trade Commission Act's[59] unfair practices clause.[60] Furthermore, the

54. *See* Cory Bennett, *OPM Letter Distances Agency from Legal Liability over Hack*, HILL (June 18, 2015), http://thehill.com/policy/cybersecurity/245457-opm-letter-distances-agency-from-legal-liability-over-hack [http://perma.cc/CK22-3VBU] (describing letter sent to breach victims disclaiming liability); Frankel, *supra* note 45 (predicting standing problems for OPM class action); Sternstein, *supra* note 12 (describing failure of past Privacy Act based cyber breach litigations). In instances where organizations may have experienced multiple security breaches, it is difficult for victims to link their harm to one specific data breach. *See* Nuala O'Connor, *Why the OPM Data Breach Is Unlike Any Other*, CDT (June 22, 2015), https://cdt.org/blog/why-the-opm-data-breach-is-unlike-any-other/ [http://perma.cc/88S7-Y4J4].

55. *See* Esworthy & Danzig, *supra* note 46 (considering court interpretation of actual damages critical); Lisa Rein, *Government Awards $133 Million Contract to Help Hack Victims, Pledging Better Customer Service*, WASH. POST (Sept. 2, 2015), http://www.washingtonpost.com/blogs/federal-eye/wp/2015/09/02/government-awards-133-million-contract-to-help-hack-victims-pledging-better-customer-service [http://perma.cc/8XQY-J4DV] (discussing $133 million already spent assisting 21.5 million people impacted). The government currently provides identity and credit monitoring, identity restoration, and identity theft insurance for OPM breach victims. *See Cybersecurity Resource Center*, OPM.GOV, https://www.opm.gov/cybersecurity/ (last visited Oct. 25, 2016) [http://perma.cc/H2ZF-4YZ8] (describing available services for victims).

56. *See* James D. Gassenheimer & Lara O'Donnell, *Heightened Expectations: Mitigating the Threat of Cybersecurity Litigation in an Ambiguous Regulatory Environment*, 57 DRI FOR DEF. 48, 50 (2015), http://www.bergersingerman.com/mobile/wp-content/uploads/2014/10/FTD-1502-Gassenheimer-ODonnell-2.pdf [https://perma.cc/2PV8-VBJ8] (discussing Federal Trade Commission's (FTC) ambiguity concerning which "reasonable measures" prevent liability). Numerous government agencies have some purview over cybersecurity in the private sector, including the FTC, Federal Bureau of Investigation (FBI), Department of Justice (DOJ), and Department of Homeland Security (DHS). *See id*. at 48-49; *see also* Davis et al., *supra* note 4, at 629 (describing the absence of regulatory uniformity surrounding data security); Rosenfeld & McDowell, *supra* note 11, at 90 (identifying how multiple regulations apply to data security).

57. 799 F.3d 236 (3d Cir. 2015).

58. *See id.* at 240. The practices that the FTC cited as unfair included: using inadequate passwords, insufficient operating systems connected to the Wyndham network, improper access by third-party vendors, and the absence of cybersecurity investigations and responses to prior attacks. *See id.* at 240-41; *see also* Gassenheimer & O'Donnell, *supra* note 56, at 50 (describing Wyndham's avoidable cybersecurity failures).

59. 15 U.S.C. §§ 41-58 (2012) (as amended).

Third Circuit held that Wyndham was entitled only to a "relatively low level of statutory notice" and therefore, had sufficient notice that it risked incurring liability through its abysmal cybersecurity measures.[61] *Wyndham* illustrates that inadequate cybersecurity risks incur private sector liability, and warns that federal regulatory agencies are willing to pursue these claims even through unwieldy avenues such as the unfair practices clause.[62]

C. S.754 and the Cybersecurity Act

On October 27, 2015, the Senate passed S.754, a bill that aims to utilize information sharing to enhance cybersecurity throughout the country.[63] Title I of S.754, CISA, directs federal agencies to develop procedures to share information about cyber threats with affected private organizations.[64] The law also allows private sector entities to voluntarily share threat information with one another or with the government.[65] Additionally, S.754 authorizes private

60. *See id.* § 45 (codifying unfair practice clause); *Wyndham*, 799 F.3d at 247-48 (establishing Wyndham's actions fell within unfair business practices definition); David J. Bender, *Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority over Corporate Data-Security Practices*, 81 GEO. WASH. L. REV. 1665, 1682 (2013) (discussing novel nature of *Wyndham* case).

61. *See Wyndham*, 799 F.3d at 255 (explaining applicable statutory notice requirement). Wyndham erroneously focused on whether the FTC had given sufficient notice of its statutory interpretation, and failed to address whether the statute gave adequate notice, which the Third Circuit held was the relevant question for the facts at hand. *See id.* The court further noted that the FTC previously issued a guidebook on cybersecurity and filed other complaints based on failed cybersecurity measures, which provided sufficient notice. *See id.* at 256-57.

62. *See* 15 U.S.C. § 45 (representing unfair practice clause of Federal Trade Commission Act); Gassenheimer & O'Donnell, *supra* note 56, at 52-53 (advising businesses of high cybersecurity standard). Commentators also advise businesses to be cognizant of a host of statutes under which they might incur liability following a cybersecurity breach. *See id.*

63. *See* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015) (describing stage and purpose of proposed legislation). The House passed a similar bill that not yet been reconciled with S.754, and President Obama issued a statement supporting S.754. *See* Andy Greenberg & Yael Grauer, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015), https://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/ [http://perma.cc/RV8C-WL9Y] (indicating additional support for S.754).

64. *See* S. 754 § 103(a) (implementing one-way sharing of information from federal agencies to public sector). Information sharing enables participants to more accurately calculate the security measures needed to rebuff a threat. *See* Trevor Ford, Comment, *Cybersecurity Legislation for an Evolving World*, 50 U.S.F. L. REV. 119, 123-24 (2016) (discussing advantages of information sharing).

65. *See* S. 754 § 104(c)(1) (establishing private entities "may" share threat information); *id.* § 104(d)(4)(B)(i) (describing explicitly voluntary nature of information flowing from private entities to government). *But see* Amie Stepanovich, *Busting the Biggest Myth of CISA—That the Program Is Voluntary*, WIRED (Aug. 19, 2015), https://www.wired.com/2015/08/access-cisa-myth-of-voluntary-info-sharing/ [http://perma.cc/K3GF-6XBQ] (alleging private sector participation in information sharing not truly voluntary). Some commentators question the utility of sharing information with government agencies that have proven incapable of protecting their own information. *See* O'Connor, *supra* note 54 (articulating concern whether federal agencies can protect information received through S.754). Nevertheless, incentives such as antitrust and trade secret protections retained on the information exchanged may encourage companies to participate in the sharing framework. *See* Frank et al., *Information Sharing Under CISA: What It Means for Companies*, LAW360 (Feb. 23, 2016), http://www.law360.com/articles/760952/information-sharing-under-cisa-what-it-means-for-comp

entities to monitor their online systems for an intrusion.[66] Interestingly, S.754 also permits the use of "defensive measures" by organizations to protect themselves from cyber attacks.[67]

S.754 requires all entities sharing cyber-threat information to remove identifying personal information from such materials.[68] Despite the textual requirements to protect personal information while sharing cyber-threat information, critics contend that S.754 does not do enough to protect private information.[69] Congress was clearly cognizant of these concerns, as S.754 requires the Privacy and Civil Liberties Oversight Board to compose a report on S.754's impact on privacy and civil liberties every two years.[70] Additionally, the head of every federal agency is required to submit detailed reports on issues relating to S.754, including the impact on "privacy and civil liberties of specific persons."[71]

S.754 leaves the question of civil liability largely unchanged and explicitly denies liability for any cause of action generated by sharing cyber-threat information under S.754.[72] S.754 permits a potential lawsuit, but only if an organization acts in a grossly negligent manner or willfully engages in misconduct while sharing cyber-threat information.[73] According to S.754,

anies [http://perma.cc/JN8K-FXRK]. The knowledge that such information may not be used against a company in an enforcement action could also incentivize company participation. *See id.*

66. *See* S. 754 § 104(a)(1)(A). Entities may also monitor another organization's system as long as that organization gives written consent. *See id.* § 104(a)(1)(B)-(C).

67. *See id.* § 104(b)(1)(A). Defensive measures, on behalf of another entity with that entity's written consent, are also authorized by S.754. *See id.* § 104(b)(1)(B)-(C). Use of defensive measures is restricted to cybersecurity purposes. *See id.* § 104(b)(1), (b)(2)(A) (identifying cybersecurity purpose of defensive measures and prohibiting defensive measures for other purposes). Some have argued that authorizing these defensive measures, which are essentially counter-measures, will only result in more conflict. *See* Jake Laperruque, *How CISA's Countermeasures Authorization Threatens Security*, CDT (July 28, 2015), https://cdt.org/blog/how-cisas-countermeasures-authorization-threatens-security/ [http://perma.cc/46AP-HUTM] (arguing defensive measures only escalate situations).

68. *See* S. 754 § 103(b)(1)(D) (stating federal agencies must restrict access to shared materials to intended recipients); *id.* § 103(b)(1)(E) (requiring government agencies to redact personal information from shared materials); *id.* § 104(d)(1) (insisting private sector sharing entities protect information exchanged); *id.* § 104(d)(2) (requiring removal of personal information from private sector shared material).

69. *See* Mike Godwin, *The Many, Many, Many Flaws of CISA*, SLATE (Oct. 26, 2015), http://www.slate.com/articles/technology/future_tense/2015/10/stopcisa_the_cybersecurity_information_sharing_act_is_a_disaster.html [http://perma.cc/Q5ZR-RTXN] (criticizing broad language of S.754 and alleging sharing information equates surveillance); Stepanovich, *supra* note 65 (considering S.754 insufficient to protect personal information). *But see* Ford, *supra* note 64, at 134-35 (arguing S.754 adequately protects personal information).

70. *See* S. 754 § 107(b)(1).

71. *See id.* § 107(a) (requiring biannual reporting of privacy issues). The agencies are also required to report the number of notices they issued to people whose privacy was infringed upon due to S.754. *See id.*

72. *See id.* § 106(a)-(b) (stating no civil liability imposed for monitoring systems or sharing threat information).

73. *See id.* § 106(c)(1) (clarifying liability scope); Robyn Greene, *Cybersecurity Information Sharing Act of 2015 Is Cyber-Surveillance, Not Cybersecurity*, NEW AM. (Apr. 9, 2015), https://www.newamerica.org/oti/cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/ [http://perma.cc/Z2EK-PNFR] (describing civil liability implications attributable to legislation).

private organizations cannot incur liability for refraining from sharing information because the bill reflects a voluntary arrangement.[74] Private companies are also protected from antitrust lawsuits when sharing information about cyber threats with one another.[75]

Title II of S.754, also known as FCEA, requires the Secretary of Homeland Security and the Director of the OMB to create a method to detect intruders in federal systems.[76] FCEA also requires the Secretary of Homeland Security to create, and offer to other federal agencies, a program that monitors federal system network traffic for cyber threats.[77] Heads of federal agencies must utilize this new system within the six months following the Secretary's development.[78]

On December 18, 2015, President Obama signed an appropriations bill that included a version of S.754.[79] Although S.754 passed into law largely unchanged from its original form, the newly enacted Cybersecurity Act contains a clause that allows the government to use and retain shared cyber-threat information to investigate or prosecute certain crimes.[80] Additionally,

74. *See* S. 754 § 108(h)(3)(i).

75. *See id.* § 104(e)(1).

76. *See* S. 754 § 228(b)(1) (demanding implementation of "intrusion assessment plan").

> [I]n response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency . . . for the purpose of protecting the information system from, or mitigating, an information security threat.

Id. § 209(h)(1)(A). In the event of an imminent threat to an agency's cybersecurity, the Secretary can implement additional "intrusion detection and prevention capabilities" to prevent a breach. *See id.* § 209(h)(2)(H)(3)(A).

77. *See id.* § 230(b)(1) (requiring implementation and distribution of monitoring system to other agencies regardless of reimbursement); *see also id.* § 204(a)(1) (requiring Secretary to provide "Continuous Diagnostics and Mitigation Program advanced security tools" within system). The Secretary is also required to test the system regularly, as well as ensure that the entire system is used for no other purpose than cybersecurity needs. *See id.* § 230(c)(4), (7).

78. *See id*. § 203(c)(1)(B) (establishing compliance deadline).

79. *See* Cybersecurity Act of 2015, Pub. L. No. 114-113, § 103, 129 Stat. 2242, 2939 (2015); *see also Omnibus Funding Bill Is a Privacy and Cybersecurity Failure: Intelligence Committees Hijacked Cyber Negotiations and Raced to the Bottom on Privacy*, NEW AM. (Dec. 16, 2015), https://www.newamerica.org/oti/omnibus-funding-bill-is-a-privacy-and-cybersecurity-failure/ [http://perma.cc/CE2H-MVTV] (considering S.754 principal source of passed act).

80. *See* Cybersecurity Act of 2015 § 105(d)(5)(A)(iii)-(v) (authorizing use of information for crimes related to physical, economic, or national harm). Some commentators characterize this particular clause as merely another way to allow government surveillance and expand the ability to search without a warrant. *See* Jadzia Butler & Greg Nojeim, *Cybersecurity Information Sharing in the "Ominous" Budget Bill: A Setback for Privacy*, CDT (Dec. 17, 2015), https://cdt.org/blog/cybersecurity-information-sharing-in-the-ominous-budget-bill-a-setback-for-privacy/ [http://perma.cc/HZ9B-J65Z] (noting alternate uses for cybersecurity information under CISA); Andy Greenberg, *Congress Slips CISA into a Bill That's Sure to Pass*, WIRED (Dec. 16, 2015), http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/ [http://perma.cc/UK

the Cybersecurity Act eliminated S.754's exclusion of liability protection for "gross negligence or willful misconduct."[81] The Cybersecurity Act also contains a sunset provision, and expires in 2025.[82]

III. ANALYSIS

A. The Cybersecurity Act's Strengths and Weaknesses

In light of the OPM data breach, as well as numerous private sector data breaches, it is clear that cybersecurity reform is needed.[83] The Cybersecurity Act's focus on cyber-threat information sharing will undoubtedly increase awareness of current cyber threats.[84] Nevertheless, it is unclear whether such information sharing would have necessarily prevented cyber breaches like the OPM data breach, caused by inadequate, low-tech security measures rather than high-tech hacking.[85]

The private sector's entirely voluntary participation in threat sharing reduces the Cybersecurity Act's effectiveness, and in practice, only requires the federal government to share threat information with the private sector.[86] This one-way flow of information is still beneficial, but hardly novel, as the EO has provided exactly this type of information sharing since 2013.[87] As a result, the Cybersecurity Act's major accomplishment appears to be little more than a codification of an existing executive order.[88]

The Cybersecurity Act grants companies permission to monitor their own

X4-E3X2] (noting CISA permits backchannel access for law enforcement). The original version in S.754 allowed non-cybersecurity related uses of shared information only for the threat of imminent crimes, but the Cybersecurity Act allows law enforcement to use the information for any threat regardless of the level of urgency. *See* Butler & Nojeim, *supra* (describing new version's information usage changes).

81. *See* John Evangelakos & Brent J. McIntosh, *A Guide to the Cybersecurity Act of 2015*, LAW360 (Jan. 12, 2016), http://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015 [http://perma.cc/L6XA-6969] (discussing elimination of explicit liability exceptions); *see also* Greene, *supra* note 73 (identifying liability issues in Cybersecurity Act).

82. *See* Cybersecurity Act of 2015 § 111(a) (identifying expiration date).

83. *See* Kesan & Hayes, *supra* note 22, at 1482 (emphasizing "urgent need" for new cybersecurity legislation); *supra* notes 2-4 and accompanying text (describing various recent data breaches).

84. *See* Teplinsky, *supra* note 10, at 279 (noting increased cyber-threat information availability assists in cybersecurity efforts); Ford, *supra* note 64, at 123 (explaining importance of information sharing).

85. *See* Major, *supra* note 6 (revealing stolen vendor credentials led to OPM breach).

86. *See* Cybersecurity Act of 2015 § 103(a) (describing public to private sector sharing); *id.* § 105 (discussing private to public sector sharing); *see also* Evangelakos & McIntosh, *supra* note 81 (describing further two-way sharing of information). Disregarding its voluntary nature, permitting private sector organizations to share cybersecurity threat information with each other is an important step. *See* Ford, *supra* note 64, at 125-26.

87. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013) (ordering government agencies to share threat information with private sector targets).

88. *Compare* Cybersecurity Act of 2015 § 103(a) (describing public to private sector sharing), *and id.* § 105 (discussing private to public sector sharing), *with* Exec. Order No. 13,636, 78 Fed. Reg. at 11,739 (mandating government agencies share threat information with private sector targets).

systems and deploy defensive measures.[89] The Cybersecurity Act defines a defensive measure as an action that "detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability," and further clarifies that permissible defensive measures exclude actions that cause substantial harm to another information system.[90] Considering the ambiguity regarding what constitutes "substantial harm," it is likely that an overzealous company could institute an aggressive defensive measure that harms another company—merely spurring more litigation.[91] A defensive measure could also blindly attack an innocent company or even a foreign government if hackers disguise their attacks by rerouting through proxies, creating further recriminations and potentially international conflicts.[92]

The Cybersecurity Act fails to clarify the civil liability issues surrounding data breaches.[93] The Cybersecurity Act even dispenses with the minor concession concerning civil liability included in S.754, which allowed lawsuits to proceed in instances of gross negligence or willful misconduct when participating in information sharing under the Cybersecurity Act.[94] All that remains in the Cybersecurity Act is the blanket shield from liability for organizations participating in the information sharing.[95]

The absence of any meaningful reform in the realm of civil liability for data breach victims is particularly significant in light of the very real and present concern that the information sharing that the Cybersecurity Act promotes will lead to additional unnecessary exposure of personal consumer information.[96] Private entities engaged in information sharing need only remove known personal information not directly related to the threat, which is an exceedingly ambiguous standard.[97] Even when used legitimately, the federal government may put shared cyber-threat information out to a wide range under the Cybersecurity Act, which raises serious privacy and surveillance concerns.[98]

89. *See* Cybersecurity Act of 2015 § 104(a)-(b).

90. *See id.* § 102(7)(A); *see also id.* § 102(7)(B) (identifying impermissible defensive measures under Cybersecurity Act).

91. *See* Ford, *supra* note 64, at 133 (acknowledging defensive measures may end in court battles); Laperruque, *supra* note 67 (noting challenges distinguishing between harm and substantial harm).

92. *See* Laperruque, *supra* note 67 (discussing potential international and domestic fallout from defensive measures).

93. *See* Greene, *supra* note 73 (discussing CISA civil liability inadequacies).

94. *See* Evangelakos & McIntosh, *supra* note 81 (describing civil liability changes between CISA and Cybersecurity Act).

95. *See* Cybersecurity Act of 2015 § 106(a)-(b) (establishing no liability exists for monitoring or sharing information). Many view the protection from civil liability for information sharing as essential to encourage participation by private companies. *See* Kelly, *supra* note 27, at 1696.

96. *See* Greene, *supra* note 73 (considering personal information shared under Cybersecurity Act unnecessary); O'Connor, *supra* note 54 (articulating concern whether federal agencies can protect information received); *see also* Frank et al., *supra* note 65 (recognizing concerns surrounding data safety). *But see* Cybersecurity Act of 2015 § 104(d)(2) (implementing personal information protections).

97. *See* Cybersecurity Act of 2015 § 104(d)(2) (describing redaction limitations).

98. *See id.* § 105(d)(5)(A) (outlining permissible uses). Under the Cybersecurity Act, information shared

Considering the Cybersecurity Act may increase consumer information's exposure to hackers, it seems particularly unjust that victims would have no clear judicial avenue to recoup their losses.[99]

Meanwhile, even without the Cybersecurity Act's broad disclaimer of liability for information sharing, victims of a government data breach continue to face difficulties in proving standing.[100] Private companies will continue to scramble to comply with multiple regulations promulgated by myriad agencies rather than a single, comprehensive statute laying out the standard to prevent liability for cyber breaches and the loss of personal consumer information.[101] The Cybersecurity Act, like its predecessor, CISA, fails to confront a central cybersecurity issue by avoiding the creation of a statutory cause of action for data breach victims to seek redress.[102]

Luckily, although Title I of the Cybersecurity Act—which is virtually identical to CISA—ultimately remains a toothless piece of legislation, Title II of the law—which mirrors FCEA—implements some much needed, common-sense reforms.[103] This portion of the Cybersecurity Act focuses on preventive measures to harden cybersecurity targets, rather than on information sharing.[104] The creation of intrusion detection, mandated encryption, and implementation of network monitoring systems are excellent steps toward ensuring the safety of government employees' personal information.[105]

B. Proposed Changes

Continued cybersecurity reform should build on FCEA's foundation and focus on incident prevention rather than information sharing.[106] Many of the recent high-profile breaches were the result of preventable low-tech security

for cybersecurity purposes can be retained and shared with federal agencies in order to investigate or prosecute a wide variety of crimes. *See id.*; *see also* Butler & Nojeim, *supra* note 80 (emphasizing permissive use of shared cyber-threat information to prosecute non-urgent threats).

99. *See* O'Connor, *supra* note 54 (mentioning sharing information exposes more personal information); *supra* notes 68-69 and accompanying text (discussing privacy concerns); *see also* Sternstein, *supra* note 12 (demonstrating victims' struggle to recoup damages from data breach).

100. *See supra* note 54 and accompanying text (describing standing issues for data breach victims).

101. *See* Davis et al., *supra* note 4, at 629 (noting absence of one comprehensive cybersecurity regulation); Rosenfeld & McDowell, *supra* note 11 (reiterating multiple regulations apply to data security).

102. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992) (explaining statutory causes of actions help elevate previously legally insufficient allegations of harm); O'Connor, *supra* note 54 (commenting on inadequacies of currently available redress).

103. *See* Cybersecurity Act of 2015 § 230(b)(1) (listing FCEA requirements); O'Connor, *supra* note 54 (advocating for common-sense reform).

104. *See* Cybersecurity Act of 2015 § 230(b)(1) (requiring implementation of detection and prevention mechanisms); *id.* § 224(a)(1) (necessitating "advanced network security tools" used by agencies); *id.* § 225(b)(1)(C) (requiring agencies to encrypt sensitive information).

105. *See supra* note 104 and accompanying text (listing FCEA security improvements).

106. *See* Sales, *supra* note 10, at 1545 (considering prevention and strengthening target's key cybersecurity components).

failings, such as unsecured passwords left unattended by employees.[107] Furthermore, OPM's systems lacked indicia of basic cybersecurity measures, such as encryption and intrusion detection.[108] Congress or NIST should take steps to implement basic necessary security measures and laws or regulations that insist on compartmentalizing critical systems from one another, thereby limiting remote access to those systems by third-party vendors and other personnel.[109]

Additionally, either Congress or NIST should ensure that personnel with actual training and experience in cybersecurity maintain each agency's compliance with security regulations.[110] Admittedly, the amended FISMA previously addressed this issue in 2014, but contemporaneous audits revealed significant failings in this area, indicating that further efforts may be necessary.[111] Real cybersecurity reform within the government requires a significant emphasis on enforcement and accountability to address the existing cybersecurity inadequacies and the previous failures to remedy them.[112] Hiring employees with cybersecurity experience and training may assist in this goal, as they have a greater grasp of the real-life consequences of an inadequately protected federal information system.[113]

Finally, Congress needs to address civil liability for cyber-breach victims.[114] The ineffective protections the federal government put in place to safeguard personal information unquestionably harmed the OPM-breach victims.[115] Congress should create a statutory cause of action for victims of both government and private sector data breaches to provide them with judicial recourse against negligence from both private and public sector agencies entrusted with the security of their information.[116] This congressional action

107. *See* Banjo, *supra* note 4 (explaining Home Depot hack resulted from stolen vendor password); Major, *supra* note 6 (revealing stolen vendor credentials led to OPM breach).

108. *See* Boyd, *supra* note 8 (attributing OPM breach to failures in encryption and intruder detection).

109. *See* Major, *supra* note 6 (emphasizing compartmentalization to minimize damage and problems posed by vendor carelessness).

110. *See* Davidson, *supra* note 7 (advocating for greater recruitment of cyber talent).

111. *Compare* Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3554(a)(3)(A) (Supp. II 2014) (mandating CIO possessing cybersecurity experience), *with* FINAL AUDIT REPORT 2014, *supra* note 6, at 5 (reporting OPM's designated security officers not properly trained).

112. *See* FINAL AUDIT REPORT 2014, *supra* note 6, at 5 (recognizing OPM's inadequate security for many years); O'Connor, *supra* note 54 (discussing continued security failings despite warnings before breach).

113. *See* Davidson, *supra* note 7 (advocating for improved recruitment of cyber talent). The federal government may have difficulty recruiting the needed talent for federal jobs because public sector jobs pay significantly less than corresponding private sector jobs in cybersecurity. *See id.*

114. *See* Greene, *supra* note 73 (considering Cybersecurity Act's civil liability scheme overly broad); O'Connor, *supra* note 54 (commenting on inadequacy of currently available redress).

115. *See supra* note 3 and accompanying text (enumerating extensive list of personal information stolen). In particular, the fingerprints stolen could be particularly compromising as technological advancement trends toward biometric identification. *See* Grande, *supra* note 3 (acknowledging personal and compromising nature of stolen fingerprints).

116. *See* Fed. Aviation Admin. v. Cooper, 132 S. Ct. 1441, 1455-56 (2012) (restricting causes of action in

would be beneficial not only to the victims, but also to organizations afraid of incurring liability under an uncertain and amorphous series of regulations.[117]

IV. CONCLUSION

Ultimately, Title I of the Cybersecurity Act does little to enhance cybersecurity through its voluntary sharing arrangement, while simultaneously raising surveillance and privacy concerns. The federal government ought to continue FCEA's preliminary work and focus on preventive measures to preclude future cyber breaches like the OPM hack. These security advancements do not require sweeping legislative reforms, rather a prioritization of cybersecurity amongst department heads. In order to prevent the recurrence of incidents like the OPM breach, department heads should focus on hiring experienced cybersecurity professionals and promoting a culture of accountability.

Unfortunately, outside the public sector, cybersecurity reform requires further legislative action. Until Congress passes legislation creating a specific cause of action for these intrusions, victims of cyber breaches will be left largely outside the reach of judicial redress. Correspondingly, this will leave private companies in the dark concerning what cybersecurity measures must be maintained in order to avoid liability. Legislation could eliminate significant confusion in the private sector, and perhaps lead to enhanced cybersecurity as a whole.

Hannah Vail

current government breaches to cases proving monetary damages); *supra* notes 53-55 (describing current difficulties for cyber breach victims bringing suit). De facto injuries that were previously insufficient may be raised to the level of concrete and "legally cognizable injuries." *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992) (noting Congress's authority to define statutory standing).

117. *See* Davis et al., *supra* note 4, at 629 (identifying absence of "united regulatory front on . . . data security"); Rosenfeld & McDowell, *supra* note 11, at 90 (noting absence of single legal data security standard).