ONCE MORE UNTO THE BREACH: THE CONSTITUTIONAL RIGHT TO INFORMATIONAL PRIVACY AND THE PRIVACY ACT

CALEB A. SEELEY*

With the rise of the internet and computer storage, the loss and theft of individuals' private information has become commonplace. Data breaches occur with increasing regularity, leading some to question if the current statutory and regulatory schemes properly incentivize the maintenance of adequate security measures amongst federal agencies. This Note argues that inadequate data security practices by government agencies implicate the constitutional right to informational privacy. While the Court has previously upheld intrusive personal information collection programs, the Privacy Act, which plays an essential role in the Court's decisions, has been weakened significantly by recent interpretation of its damages provision. Given this change in the effectiveness of the statutory protection of private data, lawsuits alleging a violation of the constitutional right to informational privacy might succeed and could help incentivize optimal levels of data security amongst government agencies.

 J.D. Candidate, 2017, New York University School of Law; B.S. 2009 Duke University. I would like to thank everyone who provided advice and feedback on this topic including Professor Florencia Marotta-Wurgler. Much thanks to all the editors of the *New York University Law Review*, especially Rich Diggs and Sarah Prostko for their immense help.

INTRODUCTION

In June 2015, the United States Office of Personnel Management (OPM) experienced data breaches that resulted in the theft of the personal information of millions of Americans.[1] The breaches affected multiple OPM computer systems and over twenty-two million people. The OPM breach has been called "one of the most damaging [breaches] on record because of its scale and, more importantly, the sensitivity of the material taken."[2] The stolen records include personally identifiable information (PII) such as Social Security Numbers, places of residence, education, and employment history.[3] What's more, the data includes detailed, and previously confidential, health, criminal, and financial records.[4]

Despite its surprising scope, the breach itself should not have come as a surprise; deficiencies in OPM's data security have been well documented.[5] An internal audit detailed "persistent deficiencies in OPM's information system security program,"[6] which indicated that "sensitive data was not secured" and "security measures were not even tested to make sure they worked."[7]

The breach exposed glaring weaknesses in the data security standards that federal agencies are responsible for implementing. The Privacy Act of 1974 (hereinafter Privacy Act, or the Act)[8] should pro-

---

[1] *See* Josh Lederman, *Biggest Breach in US History? OPM Hack Hit 21 Million People, Officials Say*, THE CHRISTIAN SCIENCE MONITOR (July 9, 2015), http://www.csmonitor.com/USA/USA-Update/2015/0709/Biggest-breach-in-US-history-OPM-hack-hit-21-million-people-officials-say (describing the breach as "the biggest in U.S. history"); Kevin Liptak, Theodore Schleifer & Jim Sciutto, *China Might Be Building Vast Database of Federal Worker Info, Experts Say*, CNN (June 6, 2015, 9:38 AM), http://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/?iid=EL (describing the severity of the breach).

[2] Patricia Zengerle & Megan Cassella, *Millions More Americans Hit by Government Personnel Data Hack*, REUTERS (July 9, 2015, 7:18 PM), http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709.

[3] *See* David Auerbach, *The OPM Breach Is a Catastrophe*, SLATE (June 16, 2015, 12:50 PM), 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.

[4] *See id.* (noting that the information extends to drug use, mental health, and salary history).

[5] *See, e.g.*, *id.* ("We *do* know that the security failings of OPM were no secret.").

[6] U.S. OFFICE OF PERS. MGMT., OFFICE OF THE INSPECTOR GEN., SEMIANNUAL REPORT TO CONGRESS: OCTOBER 1, 2014–MARCH 31, 2015, at 13 (2015), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar52.pdf.

[7] Auerbach, *supra* note 3.

[8] 5 U.S.C. § 552a (2016). The Privacy Act is "the most ambitious piece of federal legislation in the domain of information privacy," and "the most comprehensive law that regulates the processing and dissemination of information that the government collects about individuals." Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2024 (2010).

vide both secure record keeping and a civil remedy for unauthorized disclosure.[9] However, the millions of Americans whose information was stolen will have difficulty holding the agency liable due to restrictive interpretation of the Act's damages provision.[10]

After the breach, President Obama and Congress reacted quickly to prevent further harm, but they operated within the already existing regulatory framework. Congress passed the Cybersecurity Act of 2015,[11] which makes it easier for private companies to share information regarding cybersecurity threats with each other and the government.[12] President Obama has pushed to "[r]aise the [l]evel of [c]ybersecurity" across the country by allocating over $3 billion to the modernization of federal information-technology infrastructure.[13] These changes rely upon the existing statutory framework and protections of the Privacy Act. The actions create no new enforcement mechanisms or remedies for harmed individuals. In fact, the Privacy Act's framework has been extended to foreign countries and regional economic organizations.[14]

Despite these efforts to extend existing statutes and regulations, the government admits that cybersecurity is "one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[15] Noncompliance with rules has been the chief plague of data security.[16] "Federal agencies have significant weaknesses in information security controls that continue to threaten the confidentiality,

---

[9] *See* 5 U.S.C. § 552a(g) (providing civil remedies for violations of the Act).

[10] *See, e.g.*, S. Jacob Carroll, FAA v. Cooper*: Bombarding the Privacy Act with the "Canon of Sovereign Immunity*," 64 MERCER L. REV. 785, 800 (2013) (arguing Supreme Court decisions have inhibited recovery for a variety of privacy violations); Alex Kardon, *Damages Under the Privacy Act: Sovereign Immunity and a Call for Legislative Reform*, 34 HARV. J.L. & PUB. POL'Y 705, 709 (2011) ("The question of how to define actual damages may seem like a minor point, but it has real importance for the remedial efficacy of the Act.").

[11] Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N, § 1(a), 129 Stat. 2935.

[12] 6 U.S.C. § 1504 (2016) (requiring the Attorney General and Secretary of Homeland Security to publish guidance to assist private companies in sharing information).

[13] *See Fact Sheet: Cybersecurity National Action Plan*, WHITE HOUSE (Feb. 9, 2016), https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (describing President Obama's plans to allocate additional funds, take executive actions, and launch several commissions to improve cybersecurity).

[14] *See* Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (describing itself as "an act to extend Privacy Act remedies to citizens of certified states").

[15] THE WHITE HOUSE, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE 1 (2015).

[16] *See Cybersecurity*, GAO, http://www.gao.gov/key_issues/cybersecurity/issue_summary#t=0 (last visited Apr. 22, 2016) ("Despite the actions taken by several successive administrations and the executive branch agencies, significant challenges remain to enhancing the protection of cyber-reliant critical infrastructures.").

integrity, and availability of critical information and information systems."[17] Over seventy percent of major federal agencies "indicated that inadequate information security controls were either material weaknesses or significant deficiencies."[18]

While providing funds can increase agencies ability to comply with security standards, civil liability for noncompliance can encourage compliance. Liability for inadequate data security can incentivize stronger data protections and the funneling of the newly authorized money to the most-impactful sources. However, privacy law in the United States is fragmented and decreasingly coherent.[19] Additionally, the Privacy Act, the primary source of agency liability for data security, is a product of the 1970s and needs be updated to reflect the changes in technology and proliferation of computers, the Internet, and the ever-increasing collection and storage of personal information by the government.[20]

Due to the shortcomings of the Privacy Act, this Note suggests that those harmed by data breaches should look to the Constitution for the regulation of government data security. The Supreme Court's decision in *NASA v. Nelson* suggests that data collection and storage could implicate a constitutional right to privacy.[21] Meanwhile, the Court's narrow interpretation of "actual damages" in the Privacy Act in *FAA v. Cooper*[22] restricted the ability of individuals to recover damages for a violation of the Act. This Note argues that the reduction in Privacy Act liability has altered the balance of interests used to determine if the government is violating the constitutional right to informational privacy, and that the constitutional right can be used to compel adequate data security. Instead of relying on executive orders and statutes devoid of enforcement mechanisms, courts should recognize that the constitutional right to informational privacy should, at times, impose liability on the government agencies that fail to implement adequate data security measures.

This Note proceeds in three parts. Part I explores the jurisprudence and development of the constitutional right to informational

---

17 *Id.*

18 *Id.*

19 *See* Strahilevitz, *supra* note 8, at 2008 (noting divergences among the different branches of the law of privacy).

20 *See* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 380 (noting the Act has not been updated in over thirty years).

21 *See* NASA v. Nelson, 562 U.S. 134, 147 (2011) ("[W]e will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance.").

22 *See* FAA v. Cooper, 132 S. Ct. 1441, 1446 (2012) (holding "actual damages" does not include emotional harms).

privacy. Part II examines the Privacy Act and the decisions that restricted the damages provision of the Act, and it argues that the Act *now* fails to provide constitutionally required privacy protections because of the lack of damages. Part III discusses the feasibility and effectiveness of using violations of the constitutional right of informational privacy to hold federal agencies accountable for inadequate data security.

I
The Constitutional Right to Informational Privacy

The constitutional right to privacy lacks a concrete definition. This Part examines the development of the constitutional right to informational privacy that is implicated by disclosing personal information to the government. Section I.A describes the contours of the constitutional right to informational privacy. Then, Section I.B demonstrates the importance of an effective statutory protection of privacy to avoid violating the constitutional right to informational privacy.

A. Defining the Right to Informational Privacy

The Constitution does not explicitly mention a right to privacy, but the Supreme Court has recognized that "specific guarantees in the Bill of Rights" define a right of privacy, a right "older than the Bill of Rights" that forbids certain government invasions.[23] The "right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."[24] This right has been described as protecting decisional privacy, the right of individuals to "independence in making certain kinds of important decisions,"[25] and has been used by the Court as justification for striking down prohibitions of contraception,[26] abortion,[27] sodomy,[28] and more.

The Supreme Court has also grappled with a constitutional right to informational privacy grounded in the Fourteenth Amendment.[29]

---

[23] Griswold v. Connecticut, 381 U.S. 479, 484, 486 (1965).

[24] Roe v. Wade, 410 U.S. 113, 152 (1973).

[25] Whalen v. Roe, 429 U.S. 589, 599–600 (1977). These important decisions relate to marriage, procreation, contraception, family relationships, child-rearing, and education. *Id.* at 600 n.26.

[26] *Griswold*, 381 U.S. at 486.

[27] *Roe*, 410 U.S. at 152.

[28] Lawrence v. Texas, 539 U.S. 558, 578 (2003).

[29] *See* NASA v. Nelson, 562 U.S. 134, 147–48 (2011) (holding the questionnaire asking employees about treatment or counseling for recent illegal drug use did not violate the right to informational privacy, assuming such a right is protect by the Constitution); *Whalen*, 429 U.S. at 603–04 (holding that a statute which required a state to be provided

Scholars describe the right as protecting a distinct but related concept—the freedom from having private affairs made public by the government.[30] In *Whalen v. Roe*, the Court acknowledged that the right to informational privacy is "implicit in the concept of ordered liberty" and likely protected by the Fourteenth Amendment.[31]

The Supreme Court has never held that the freedom from disclosure component of the right to privacy is protected by the Constitution. In the three cases where the Court addresses the informational right to privacy, it acknowledges "that the disclosure of private information to the State [is] an unpleasant invasio[n] of privacy."[32] However, it refrained from ruling on the existence of the right, instead, repeatedly "assum[ing], without deciding, that the Constitution protects a privacy right of [this] sort."[33] The Court "referred broadly to a constitutional privacy 'interest in avoiding disclosure of personal matters.'"[34] As the Court has stated, cases protecting privacy have involved "at least two different kinds of interests," including both an "interest in avoiding disclosure of personal matters" and an interest in "making certain kinds of important decisions" without government interference.[35]

In each case dealing with the right of informational privacy, the Supreme Court applies a balancing test to determine the scope of the right by weighing the individual interest in privacy against the govern-

---

with a copy of every prescription for certain drugs did not violate the right to informational privacy); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457–65 (1977) (holding the Presidential Recordings and Materials Preservation Act did not impermissibly infringe on former presidents' privacy interests); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 530 (2006) (explaining that *Whalen* "recognized that the 'right of privacy' [was] based on substantive due process").

[30] Philip B. Kurland, *The Private I: Some Reflection on Privacy and the Constitution*, *in* TAKING THE CONSTITUTION SERIOUSLY: ESSAYS ON THE CONSTITUTION AND CONSTITUTIONAL LAW 282, 284 (Gary L. McDowell ed., 1981).

[31] *Whalen*, 429 U.S. at 599 n.23; *Roe*, 410 U.S. at 153. The *Whalen* Court emphasized that the constitutional privacy right does not emanate from the Fourth Amendment and is distinct from private affairs made public as the result of a search or seizure by the government. *Whalen*, 429 U.S. at 604 n.32. The Fourteenth Amendment provides, in part, that citizens of the United States shall not be deprived of liberty without due process of law. U.S. CONST. amend. XIV, § 1.

[32] *Nelson*, 562 U.S. at 145 (internal quotation marks and citation omitted).

[33] *See id.* at 138 ("[W]e will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance."); *Whalen*, 429 U.S. at 605–06 ("We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional."); *Nixon*, 433 U.S. at 457–58 ("We may assume with the District Court, for the purposes of this case, that this pattern of *de facto* Presidential control and congressional acquiescence gives rise to appellant's legitimate expectation of privacy in such materials.").

[34] *Nelson*, 562 U.S. at 138 (quoting *Whalen*, 429 U.S. at 599–600).

[35] *Whalen*, 429 U.S. at 599.

ment's interest in the challenged action.[36] The Court has not given guidance on the level of scrutiny, but has "reject[ed] the argument that the Government, when it requests job-related personal information . . . has a constitutional burden to demonstrate that its questions are 'necessary' or the least restrictive means of furthering its interests."[37]

The circuit courts have been less reticent, explicitly acknowledging the right to informational privacy that can be violated when an individual's legitimate expectation of privacy outweighs the state's need for information.[38] Most of the circuit courts have held that disclosure of at least some categories of personal information—such as information about one's mental or physical health—should be subject to a test that balances the government's interest in collecting confidential information against the individual's interest in avoiding its disclosure.[39] The "confidentiality branch of the right to privacy" is

---

[36] *See Nixon*, 433 U.S. at 458 ("[A]ny intrusion must be weighed against the public interest."); *Whalen*, 429 U.S. at 598–600 (weighing the "State's vital interest in controlling the distribution of dangerous drugs" against the individual's "interest in the nondisclosure of private information"); *Nelson*, 562 U.S. at 147 (announcing the court is following the same approach that it took in *Whalen*). Circuit courts have also followed the balancing approach. *See, e.g.*, *In re* Crawford, 194 F.3d 954, 959 (9th Cir. 1999) ("[P]recedents demand that we 'engage in the delicate task of weighing competing interests' to determine whether the government may properly disclose private information." (quoting United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980))); Borucki v. Ryan, 827 F.2d 836, 848 (1st Cir. 1987) ("Most of the courts finding a right of confidentiality had used a balancing test to assess violations of that right.").

[37] *Nelson*, 562 U.S. at 153. Justice Brennan originally suggested that a deprivation of privacy would only be constitutional "if it were necessary to promote a compelling state interest." *Whalen*, 429 U.S. at 607 (Brennan, J., concurring). However, to date, the Court has not adopted this minority opinion. *See Nelson*, 562 U.S. at 153.

[38] *E.g.*, Kallstrom v. City of Columbus, 136 F.3d 1055, 1064 (6th Cir. 1998) ("Where state action infringes upon a fundamental right, such action will be upheld under the substantive due process component of the Fourteenth Amendment only where the governmental action furthers a compelling state interest, and is narrowly drawn to further that state interest."); Lyle v. Dedeaux, No. 94-60200, 1994 WL 612506, at *6 (5th Cir. Oct. 24, 1994) (holding that a disclosure of personal information does not violate a person's right to privacy unless the person's legitimate expectation of privacy outweighs a legitimate state need for the information); Kelly v. City of Sterling Heights, No. 90-1895, 1991 WL 207548, at *2 (6th Cir. Oct. 16, 1991) ("A privacy interest is not constitutionally protected unless it relates to sensitive, personal, and private information which warrants confidentiality."); Flanagan v. Munger, 890 F.2d 1557, 1570 (10th Cir. 1989) ("The Supreme Court has recognized that the constitutional right to privacy protects an individual's interest in preventing disclosure by the government of personal matters."); Mangels v. Pena, 789 F.2d 836, 839 (10th Cir. 1986) ("Due process thus implies an assurance of confidentiality with respect to certain forms of personal information possessed by the state. Disclosure of such information must advance a compelling state interest which, in addition, must be accomplished in the least intrusive manner.").

[39] *See In re* Crawford, 194 F.3d at 959 ("[T]he government has the burden of showing that 'its use of the information would advance a legitimate state interest and that its actions are narrowly tailored to meet the legitimate interest.' "(quoting Doe v. Attorney Gen., 941

protected by "the Court's recognition that some form of scrutiny beyond rational relation is necessary to safeguard the confidentiality interest."[40] The Third Circuit enumerated factors courts should consider when balancing these interests, including: "the type of record requested, the information it does or might contain, the potential for harm" from "nonconsensual disclosure," the injury from disclosure, the need for access, whether there is public interest militating toward access, and, importantly, the *adequacy of safeguards* to prevent unauthorized disclosure.[41]

The Court has given the government's interest in collecting data on its employees a substantial weight in the balancing test. The Court has expressly relied on the greater freedom[42] the government has to deal with citizen-employees to justify the collection of expansive swaths of personal information. The Court found the government to be similar to private employers who regularly conduct background checks on potential employees.[43] This provides an increased government interest in invading the privacy of applicants and employees.[44]

An example of a court using the right of informational privacy to limit the collection of information is *Fraternal Order of Police, Lodge*

F.2d 780, 796 (9th Cir. 1991))); Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) ("Individuals who are infected with the HIV virus clearly possess a constitutional right to privacy regarding their condition."); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980) ("Information about one's body and state of health is matter which the individual is ordinarily entitled to retain within the private enclave where he may lead a private life."). The Sixth and Eighth Circuits have recognized a more limited informational privacy right. *See* Alexander v. Peffer, 993 F.2d 1348, 1350 (8th Cir. 1993) ("[T]o violate [the] constitutional right of privacy the information disclosed must be either a shocking degradation or an egregious humiliation of [the plaintiff] to further some specific state interest, or a flagrant breach of a pledge of confidentiality which was instrumental in obtaining the personal information."); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (holding that the right to informational privacy protects against intrusions upon interests "that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty'" (quoting McElrath v. Califano, 615 F.2d 434, 441 (7th Cir. 1980))). The D.C. Circuit, on the other hand, has refused to "enter the fray" and expressed grave doubts that any constitutional right to informational privacy exists. Am. Fed'n of Gov't Emps. v. U.S. Dep't of Hous. & Urban Dev., 118 F.3d 786, 793 (D.C. Cir. 1997).

[40] Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983).

[41] *Westinghouse*, 638 F.2d at 578.

[42] *Nelson*, 562 U.S. at 148–49 ("Government has a much freer hand in dealing 'with citizen employees than it does when it brings its sovereign power to bear on citizens at large.'" (quoting Engquist v. Or. Dep't of Agric., 553 U.S. 591, 599 (2008))).

[43] *Id.* (discussing how the questions asked as part of the background check were "part of a standard employment background check of the sort used by millions of private employers").

[44] *Id.* at 148 ("When the Government asks respondents and their references to fill out [OPM forms], it does not exercise its sovereign power 'to regulate or license.' Rather, the Government conducts the challenged background checks in its capacity 'as proprietor' and manager of its 'internal operation.'" (quoting Cafeteria & Rest. Workers v. McElroy, 367 U.S. 866, 896 (1961))).

No. 5 v. City of Philadelphia.[45] In this case, the Third Circuit considered a questionnaire the Philadelphia Police Department provided to applicants to the Special Investigation Unit.[46] The police union sought an injunction, alleging that the questions infringed on the officer's federal constitutional right of privacy.[47] The court applied "a flexible balancing approach," weighing the privacy interest in the gathered personal medical information against the government's interest in disclosure.[48] The court held that questions relating to drug use and mental health did not violate the officers' privacy since "the medical information requested is directly related to the interest of the police department in selecting officers."[49] Additional questions disclosing financial information, gambling, and alcohol consumption were similarly justified by the significant government interest.[50] However, the court identified "the adequacy of safeguards to prevent unauthorized disclosure" as one of the "crucial factors in weighing the competing interests," and found "a complete absence" of protections of the confidential personal information.[51] With "no statute or regulation that penalizes officials," the court upheld the injunction forbidding the questionnaire and required the city to "establish[ ] written, explicit, and binding rules that contain adequate safeguards against unnecessary disclosure of the confidential information."[52]

B. The Role of the Privacy Act

In *Nelson*, the Supreme Court relied on the Privacy Act as an adequate safeguard against disclosure while upholding the constitutionality of background check forms.[53] *Nelson* involved a suit by contract employees of the Jet Propulsion Laboratory who alleged that requiring federal employees to complete a background check was unlawful.[54] According to the Court, most of the questions on these forms were inoffensive, but some, including the "group of questions concerning illegal drug[ ] [use] required closer scrutiny."[55] After assuming that the challenged forms implicate a right to privacy of con-

---

[45] 812 F.2d 105 (3d Cir. 1987).
[46] *Id.* at 107.
[47] *Id.* at 108.
[48] *Id.* at 110–16.
[49] *Id.* at 114.
[50] *Id.* at 116.
[51] *Id.* at 117–18.
[52] *Id.*
[53] NASA v. Nelson, 562 U.S. 134, 147–48 (2011) (holding that the right to informational privacy was not violated by employee background checks).
[54] *Id.* at 142.
[55] *Id.* at 143.

stitutional magnitude, the Court held that "whatever the scope of [the right of informational privacy], it does not prevent the Government from asking reasonable questions of the sort included on [the required forms] in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure."[56]

The Privacy Act's central role in *Nelson* is consistent with the Court's reliance on statutory protections of personal information as fundamental to the balancing of interest in previous cases. In *Whalen*, the Court faced a challenge to a statutory scheme promulgated by New York City that required physicians prescribing certain drugs to send a form to the state identifying the patient who received the prescription.[57] The Court acknowledged that the disclosure of "private information" to the State was an "unpleasant invasion[ ] of privacy," but the Court asserted that the New York City statute contained security provisions that protected against "[p]ublic disclosure of patient information."[58] This kind of "statutory or regulatory duty to avoid unwarranted disclosures" of "accumulated private data" was sufficient, in the Court's view, to protect a privacy interest that "has its roots in the Constitution."[59] Additionally, in *Nixon*, the Supreme Court upheld a statute requiring the preservation and review of presidential recordings despite the "legitimate expectation of privacy in such material."[60] Again, the privacy interest was countered by a statutorily required process that instituted precautions to "prevent[ ] undue dissemination of private materials."[61] Thus, the constitutional right to privacy under the Fourteenth Amendment depends, in part, on the Privacy Act's protections of the personal information the government collects.

Lawful collection of sensitive personal information by government agencies depends, in part, on the Privacy Act's protections.

---

[56] *Id.* at 147–48.

[57] Whalen v. Roe, 429 U.S. 589, 591 (1977).

[58] *Id.* at 600–01.

[59] *Id.* at 605–06.

[60] Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 458 (1977).

[61] *Id.* The importance of security measures also permeates the circuit court jurisprudence. *See* Am. Fed'n of Gov't Emps. v. U.S. Dep't of Hous. & Urban Dev., 118 F.3d 786, 793 (D.C. Cir. 1997) (holding that the Privacy Act requires records to be maintained under secure conditions, and that "where the government has enacted reasonable devices to secure the confidentiality of records we cannot, without grounds, assume that the devices will prove insufficient"). Additionally, the Privacy Act affects the balancing of individual and government interests since the Act is a statutory barrier to dissemination. *Id.* ("[T]he individual interest . . . is significantly less important where the information is . . . not disseminated publicly."). Lacking "evidence that the security provisions would prove insufficient[,] . . . [an] unsubstantiated fear of public disclosure [is] not a sufficient reason for invalidating [a] statute." *Id.*

After the decision in *Nelson*, the Court severely restricted the effectiveness of the Privacy Act with its decision in *Cooper*—potentially altering the balance of interests at play when the government collects data. As noted by Justice Scalia, "the Privacy Act is necessary to [*Nelson*'s] holding."[62] The precedents demonstrate a "statutory or regulatory duty to avoid unwarranted disclosures" is central to dispelling privacy concerns,[63] with the Court holding that the requirements of the Privacy Act "give 'forceful recognition' to a [citizen's] interest in maintaining the 'confidentiality of sensitive information . . . in his personnel files.'"[64] Thus, the data security mandated by the Privacy Act, which is essential to preventing undue dissemination of information, is evidence of "'a proper concern' for individual privacy."[65]

II
The Narrowing of the Privacy Act

The Privacy Act was passed by Congress in the wake of the Watergate scandal in order to regulate the treatment of personal information by the federal government, and protect the privacy rights of American citizens.[66] Central to those protections, the Act requires that agencies "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[67] More generally, the Act places requirements on government agencies that maintain records of individuals,[68] and provides those individuals with rights to take affirma-

---

[62] NASA v. Nelson, 562 U.S. 134, 167 (2011) (Scalia, J., concurring).

[63] *Whalen*, 429 U.S. at 605; *Nixon*, 433 U.S. at 458–65 (rejecting the defendant's claim that his privacy was violated in part because the statute in question provided safeguards against "undue dissemination" of his private materials).

[64] *Nelson*, 562 U.S. at 156 (quoting Detroit Edison Co. v. NLRB, 440 U.S. 301, 318 n.16 (1979)).

[65] *See id.* (quoting *Whalen*, 429 U.S. at 605).

[66] "If we have learned anything [from] Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom." 120 Cong. Rec. S6741 (daily ed. May 1, 1974) (statement of Sen. Ervin), *reprinted in* Legislative History of the Privacy Act of 1974: Source Book on Privacy 4 (Joint Comm. on Gov't Operations ed., 1976); *see also* John F. Joyce, *The Privacy Act: A Sword and a Shield but Sometimes Neither*, 99 Mil. L. Rev. 113, 122 (1983) ("The Watergate scandal which created a political crisis unparalleled in the history of this country also kindled a firestorm of interest in the protection of personal privacy from governmental intrusions.").

[67] 5 U.S.C. § 552a(e)(10) (2012).

[68] § 552a(e).

tive steps to ensure that their information is adequately protected.[69] The Act enables individuals to access personal records stored by the government,[70] request corrections to inaccurate information,[71] ask for administrative review of agency decisions on a correction request[72] and, vitally, bring civil lawsuits for any failure by the government to comply with the Act that results in an "adverse effect."[73]

However, as a result of recent interpretation of the Act's text, the ability of its civil liability provisions to enforce the statutory privacy protections Congress promised the American people is in doubt.[74] The Supreme Court has narrowly defined the damages provision of the Act,[75] drastically limiting the situations that result in government liability. Section II.A describes the regulatory framework imposed by the Privacy Act. Section II.B examines the protections Congress intended the Act to provide. Section II.C follows the Court's narrowing of the Act's civil liability provision, culminating with the elimination of recovery for emotional damages in *Cooper*. Finally, Section II.D looks at the challenges facing individuals whose data was stolen in the OPM breach and argues that the restrictions on recovery of damages have undermined the Act's original protections.

A. Liability Under the Privacy Act

Congress passed the Privacy Act in response to public alarm over the federal government's increasing collection of private information.[76] The Act places a number of limitations on federal agencies' abilities to disclose, maintain, collect, and use information.[77] Specifically, a federal agency may not disclose any records unless the disclosure is made because of a written request by, or with written consent from, the individual to whom the record pertains.[78] Detailed accounts

---

[69] § 552a(d).

[70] § 552a(d)(1).

[71] § 552a(d)(2).

[72] § 552a(d)(3).

[73] § 552a(g)(1)(D).

[74] *See* discussion *infra* Sections II.C–II.D (discussing the Court's restrictive interpretation of "actual damages" and its effect on remedies).

[75] *See* FAA v. Cooper, 132 S. Ct. 1441, 1456 (2012) (holding "actual damages" does not include emotional harms); Doe v. Chao, 540 U.S. 614, 616 (2004) (holding an individual must show actual damages and not just an adverse effect in order to recover the statutory minimum award).

[76] *Cf.* Joyce, *supra* note 66, at 118 (detailing concerns over "the increasing computerization of sensitive personal data, the continuing sophistication of technology, and the alarming tendency of the government to put information technology to uses detrimental to individual privacy").

[77] § 552a(b)–(f).

[78] § 552a(b).

of disclosures must be kept by the agency.[79] An agency must ensure the accuracy of all records before any disclosure,[80] and individuals are given the right to access records and correct inaccuracies.[81]

Additionally, to compel and enforce the protection of collected data, the Act requires that the agencies "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[82]

Civil enforcement is essential to the effectiveness of the Act.[83] At least one scholar claims Congress believed federal agencies would have minimal incentives to enforce the Privacy Act, and aimed to provide for the "widest possible citizen enforcement."[84] It appears Congress viewed the civil remedies as an essential component of the Act's enforcement scheme.[85] Anytime an agency fails to comply with any provision of the Act in such a way as to have an "adverse effect on an individual,"[86] and a court determines the violation was "intentional or willful," the United States is liable for the amount of "actual damages sustained by the individual."[87] To enforce these requirements, the government has expressly waived its sovereign immunity to civil lawsuits under the Act,[88] endorsing the theory that private enforcement will compel agencies to adhere to the Act's mandate and protect individuals' privacy.[89] Importantly, injunctive relief is not authorized when a suit is maintained under the damages provision, leaving the deterrent effect of damages as the sole means of encouraging agency

---

[79] § 552a(c).

[80] § 552a(e)(6).

[81] § 552a(d).

[82] § 552a(e)(10).

[83] *See* Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 103 (2005) ("Recognizing that federal agencies have little incentives to enforce the Privacy Act, Congress intended to provide incentives for the 'widest possible citizen enforcement.'" (quoting S. REP. NO. 93-1183, at 83 (1974))); Frederick Z. Lodge, Note, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 FORDHAM L. REV. 611, 619–22 (1984) (arguing "[t]he civil-damages remedy was perceived by Congress as a vital element of the Privacy Act's enforcement scheme").

[84] *See, e.g.*, Hong, *supra* note 83, at 104 (arguing that "government agencies fail to protect personal privacy because they have no incentives to protect privacy").

[85] *See* Lodge, *supra* note 83, at 619–22 (noting "the broad range of potential bases of civil liability created by Congress" in the Act).

[86] § 552a(g)(1)(D).

[87] § 552a(g)(4).

[88] § 552a(g)(1).

[89] *See* Lodge, *supra* note 83, at 611–12 (arguing that the Act is "self-enforcing through its remedial provisions").

compliance.[90] Where the agency acted in an intentional or willful manner, and the plaintiff can show both an adverse effect and a causal connection between the Privacy Act violation and the plaintiff's injuries, the Act allows successful plaintiffs to recover monetary damages.[91]

Courts have repeatedly affirmed both the importance of civil liability and the requirement that agencies establish adequate data security. For example, courts have held that agencies lack the statutory authority to exempt records from the civil liability provision of the Privacy Act, as permitting such an exemption would run contrary to the purpose of the Privacy Act.[92] Despite a range of exceptions to the requirements of the Act,[93] no agency is permitted to exempt themselves from the requirement of establishing adequate data security.[94]

B. The Adequate Security Requirement

The threat of liability for violations of the Act is integral to the requirement that agencies adequately protect the data they collect. The text of the Privacy Act expressly requires that agencies establish appropriate safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[95] The Act then

---

[90] FAA v. Cooper, 132 S. Ct. 1441, 1459 n.4 (2012) (Sotomayor, J., dissenting).

[91] § 552a(g)(4).

[92] *See* Tijerina v. Walters, 821 F.2d 789, 797 (D.C. Cir. 1987) ("The interpretation offered by the government would give agencies license to defang completely the strict limitations on disclosure that Congress intended to impose."); Nakash v. U.S. Dep't of Justice, 708 F. Supp. 1354, 1360 (S.D.N.Y. 1988) (calling the idea that an agency could exempt itself from civil liability a "disturbing possibility"). Both the House and Senate wanted to protect individuals by encouraging private enforcement of the Act. *See* Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 965–66 (1991) (explaining that both the initial drafts of the Act in both chambers and the final version allowed for private enforcement).

[93] § 552a(b). The Act also provides for general and specific exemptions from requirements if the head of an agency promulgates a rule to that effect. § 552a(j)–(k). This includes the CIA and any agency "which performs as its principal function any activity pertaining to the enforcement of criminal laws." § 552a(j).

[94] Section 552a(j) does not allow agencies to opt out of § 552a(e)(10). § 552a(j). Even agencies pertaining to the enforcement of criminal laws must comply with the Act's requirement for the establishment and maintenance of adequate data security, despite broad exemptions from the Act's other requirements. *Id.*

[95] § 552a(e)(10).

allows civil suits for a violation of this provision, which should allow for citizen enforcement of the adequate safeguard requirement.[96]

Congress intended for agencies to adopt "'appropriate safeguards' [that] should incorporate a standard of reasonableness and 'refer to those safeguards which represent current state-of-the-art procedures at any given time, despite any weaknesses that may exist in the technology at that time.'"[97] The Act was meant to protect against the rapidly increasing threat of data breaches in coming years.[98] Congress mandated a reasonable level of security to incentivize "increasingly higher standards of 'reasonableness' as new technologies are further developed to make our systems progressively more secure"[99] through an affirmative burden on agencies.[100]

Additionally, the requirement that the agency act in a manner that is "intentional or willful"[101] does not prevent the Act from being used to enforce the requirement of adequate data security. When disclosures occur after the agency is aware of prior failings, the failure to establish appropriate safeguards has been found intentional and willful.[102] The accumulation of various breakdowns and misconduct can lead to the inference that the agency willfully failed to establish adequate safeguards to protect records.[103] Courts have held agencies responsible where a "loop-hole in the security system made it possible . . . to [cause] substantial[ ] harm" by accessing a system without

---

[96] § 552a(g)(1)(D) ("Whenever any agency . . . fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency.").

[97] S. REP. NO. 93-1183, at 54 (1974), *as reprinted in* 1974 U.S.C.C.A.N. 6916, 6969.

[98] *Id.* at 55 ("Both managers and policymakers should be aware that the payoff in sensitive personal information to be obtained by . . . outsiders breaching system security is going to increase in the coming years. More comprehensive information about people will be collected in the kind of large-scale record systems that are growing up.").

[99] *Id.* at 54. Aware that grounding protections on a standard of "reasonableness" could result in stagnation in the adoption of new technologies, the report specifically expressed that the Act is not "intend[ed] to discourage the active pursuit of new and more useful safeguards." *Id.*

[100] *Id.* ("[A]gencies would be expected, in compliance with the Act, to seek [security] features where necessary.").

[101] § 552a(g)(4).

[102] *See* Pilon v. U.S. Dep't of Justice, 796 F. Supp. 7, 12–13 (D.D.C. 1992) (finding the "intentional or willful" requirement satisfied where the Department of Justice was "aware of several prior disclosures regarding this plaintiff and several requests for investigation and corrective action").

[103] *See* Ciralsky v. CIA, 689 F. Supp. 2d 141, 159 (D.D.C. 2010) ("If the [Agency's] handling of Plaintiff's records involved various breakdowns and misconduct as alleged . . . then it can be plausibly inferred that the [Agency] did not properly establish rules of conduct for and provide instruction . . . as required by § 552a(e)(9), or else the failures would not have occurred.").

detection.[104] Where there is evidence that it is "widely known" that an agency's security is inadequate and "confidentiality and security are significantly jeopardized," the security failure satisfies the willful and intentional requirement of the Act.[105]

American Federation of Government Employees v. Hawley[106] demonstrates how the Privacy Act penalized agencies that failed to institute adequate data security when courts considered emotional harms to be "actual damages."[107] The Transportation Security Administration (TSA) noticed that a hard drive containing personnel data for nearly 100,000 employees—including names, social security numbers, birth dates, payroll information, financial allotments, and bank account and routing information—was missing.[108] In response, the plaintiffs, four TSA security officers, filed a complaint alleging a violation of the Privacy Act due to the inadequacy of TSA's data security.[109] The court held that the complaint satisfied the requirement that the violation of the Privacy Act was committed "in an intentional or willful manner" because "a finding that defendants were warned of the deficiencies in their information security but failed to establish proper safeguards" indicated that TSA "flagrantly disregard[ed] others' rights under the Act."[110] Additionally, the court held that the plaintiffs suffered an adverse effect and actual damages under the Act by alleging emotional harms.[111] The plaintiffs were not required to plead current, actual, pecuniary loss before the court because *Hawley* was decided before the Supreme Court limited "actual damages" to pecuniary harms in *Cooper*.[112]

Even with no evidence of resultant identity theft, TSA was held accountable for their inadequate data security. The court's ruling, which depended on emotional harms counting as "actual damages,"[113] led the TSA to settle the claims for twenty million dollars, compen-

104 Schmidt v. U.S. Dep't of Veterans Affairs, 218 F.R.D. 619, 634 (E.D. Wis. 2003).

105 *Id.* at 634–35.

106 543 F. Supp. 2d 44 (D.D.C. 2008).

107 *Id.* at 53.

108 *Id.* at 45.

109 *Id.*

110 *Id.* at 51–52.

111 *Id.* at 52–53 (indicating that plaintiffs who allege they must take "affirmative steps to recover peace of mind, emotional stability, and personal security, including but not limited to, frequently obtaining and reviewing credit reports, bank statements, and other similar information" have satisfied the requirement of showing they suffered "actual damages").

112 *See infra* Section II.C (describing the Court's interpretation of "actual damages" in *Chao* and *Cooper*).

113 *Hawley*, 543 F. Supp. 2d at 53.

sating the victims of the breach while holding the Agency accountable for its porous security.[114]

Thus, before the Supreme Court's restriction of the definition of "actual damages," the Privacy Act authorized private enforcement of data security through civil suits for failures to implement adequate or reasonable security measures.[115] The Act originally allowed individuals to be compensated for the loss of their PII, while serving to incentivize adequate security practices on the part of agencies, placing the actor in the best position to protect the data with legal liability for that failure.[116] In this way, the Act encouraged the "immediate application of all of these techniques [that] can contribute . . . to better protection of data confidentiality and individual privacy,"[117] promoting adequate security of personal data that the Court relied on in *Nelson*.[118]

C. The Supreme Court's Narrow Interpretation of "Actual Damages"

Despite the importance of civil liability to accomplish the purpose of the Privacy Act, "[t]he text of the damages provision provide[d] little guidance on the scope of 'actual damages' under the Act,"[119] and has been interpreted by the Supreme Court—first in *Doe v. Chao*[120]

---

[114] *See, e.g.*, A. Michael Froomkin, *Government Data Breaches*, 24 BERKELEY TECH. L.J. 1019, 1035 (2009) (noting that the adverse preliminary ruling "was enough to motivate the TSA to settle the plaintiffs' claims for twenty million dollars. . . ."); Terry Frieden, *VA Will Pay $20 Million to Settle Lawsuit Over Stolen Laptop's Data*, CNN (Jan. 27, 2009), http://www.cnn.com/2009/POLITICS/01/27/va.data.theft/?iref=mpstoryview.

[115] *See* 5 U.S.C. § 552a(g)(1)(D) (2012) (authorizing damages where an agency "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual," which includes the establishment of appropriate safeguards under § 552a(e)(10)).

[116] According to some scholars, the optimal allocation of resources requires courts to assign liability to the party who can avoid the costs most cheaply. *See, e.g.*, GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 19 (1970) (discussing the ability of courts to prevent the need for costly market transactions by properly allocating legal rights); R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 16 (1960) (discussing the legal system's ability to allocate rights to "achieve the same result at less cost than would be incurred by using the market").

[117] S. REP. NO. 93-1183, at 55 (1974), *as reprinted in* 1974 U.S.C.C.A.N. 6916, 6969.

[118] *See supra* Section I.B.

[119] Kardon, *supra* note 10, at 736; *see also* FAA v. Cooper, 132 S. Ct. 1441, 1449 (2012) ("[T]he meaning of 'actual damages' is far from clear."); Johnson v. Dep't of Treasury, 700 F.2d 971, 974 (5th Cir. 1983), *abrogated by* Doe v. Chao, 540 U.S. 614 (2004) (asserting that "'actual damages' has no plain meaning or consistent legal interpretation"); Fitzpatrick v. IRS, 665 F.2d 327, 329 (11th Cir. 1982), *abrogated by* Doe v. Chao, 540 U.S. 614 (2004) ("'[A]ctual damages' has no consistent legal interpretation."); Lodge, *supra* note 83, at 612 ("The term 'actual damages' . . . has no generally accepted legal definition, and is not clearly defined in the Privacy Act.").

[120] 540 U.S. 614 (2004).

and then again in *FAA v. Cooper*[121]—in ways that restrict recovery. The Court's narrow reading of "actual damages" has led some to argue that the Court has rendered the Act "toothless."[122]

First, in *Chao*, the Court held that a violation of the Privacy Act resulting in an "adverse effect[ ]" on an individual was not sufficient, without more, to recover damages.[123] Instead, plaintiffs must show not only that there has been an "intentional or willful violation of the Act producing some adverse effect," but also that they have suffered some provable "actual damages" before they can recover the statutory minimum of $1000.[124]

Petitioner Buck Doe's allegation that the disclosure of his Social Security number resulted in emotional distress proved unconvincing to the Court.[125] While the Department of Labor admittedly violated the Privacy Act by using Doe's Social Security number to identify his benefits claim, the lack of corroborative evidence for Doe's assertion of emotional distress precluded recovery.[126] Doe indicated that he was "'torn . . . all to pieces' and 'greatly concerned and worried' because of the disclosure of his Social Security number and its potentially 'devastating' consequences."[127] Yet, because he failed to provide evidence of physical symptoms or medical treatment to support his alleged distress, Doe's claim was sufficient to show an "adverse effect" under the Act, but not sufficient to allow him to recover the statutory minimum damages because the concern and worry he experienced did not qualify as "actual damages."[128]

Accordingly, the Court established the critical nature of "actual damages" to the Privacy Act's damages provision. While the definition of "adverse effect" was interpreted to be "a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing,"[129] the Court held that eligibility for damages is "confined . . . to victims of adverse effects caused by intentional or willful actions," and who suffer "actual damages."[130] Following *Chao*, a violation of the Act was no longer sufficient to generate liability since "general damages are not authorized for a statu-

121 132 S. Ct. 1441 (2012).
122 *E.g.*, Kardon, *supra* note 10, at 767.
123 540 U.S. at 620.
124 *Id.* at 627.
125 *Id.* at 617–18.
126 *Id.*
127 *Id.*
128 *Id.*
129 *Id.* at 624.
130 *Id.* at 620.

tory violation."[131] Although the specific definition of what kinds of damages fall under the definition of "actual damages" was left "for another day," the court was unequivocal that "presumed damages are . . . clearly unavailable."[132] The Court's interpretation increased the hurdles for individuals seeking to recover damages from violations of the Privacy Act and insulated agencies who failed to comply with the Act.[133]

A year after *Nelson* upheld the constitutionality of OPM's data collection based on the Privacy Act's privacy protections,[134] the Court made it even more difficult for individuals to recover under the Act. The Court in *FAA v. Cooper* addressed the division among the circuit courts on the meaning and scope of the term "actual damages," holding that the definition of "actual damages" does not include emotional harms, and is only limited to provable pecuniary harms.[135]

In *Cooper*, respondent Stanmore Cooper alleged that the unlawful disclosure of his HIV positive status "caused him 'humiliation, embarrassment, mental anguish, fear of social ostracism, and other severe emotional distress.'"[136] Despite the district court's finding that the agency's behavior was unlawful,[137] Cooper was unable to recover for emotional distress without providing evidence of pecuniary damages.[138]

The Court held that the civil remedy provision does not authorize awards for mental or emotional distress because "actual damages" is an ambiguous term that must be construed narrowly in light of the cannon of sovereign immunity.[139] The Court declared that while it is "clear from the statute" that "Congress has consented to be sued for damages under the Privacy Act," the scope of the waiver of sovereign immunity was unclear.[140] Finding ambiguity in the term "actual damages," the Court construed all ambiguity against finding a waiver of sovereign immunity by the government.[141] The Court held that "actual damages" should be interpreted "as the equivalent of special damages" from tort defamation cases, which require a showing of

131 *Id.* at 622.

132 *Id.*

133 *See* Hong, *supra* note 83, at 98 (arguing that the decision in Doe decimated private enforcement of the Privacy Act).

134 *See supra* Section I.B.

135 132 S. Ct. 1441, 1456 (2012).

136 *Id.* at 1447.

137 Cooper v. FAA, 816 F. Supp. 2d 778, 790 (N.D. Cal. 2008), *rev'd*, 622 F.3d 1016 (9th Cir. 2010), *rev'd*, 132 S. Ct. 1441 (2012).

138 *Id.* at 792.

139 *Cooper*, 132 S. Ct. at 1456.

140 *Id.* at 1448.

141 *Id.*

pecuniary harm and does not include general emotional or reputational injury.[142] Thus, mental and emotional harms—even when potentially severe and debilitating—are not recoverable unless the harm "can be substantiated by proof of tangible economic loss."[143]

Together, the holdings of *Chao* and *Cooper* have severely limited the types of Privacy Act violations that will result in liability for the offending agency, confirming scholars' fears that "[a] narrow reading of actual damages would compound the damage-limiting nature of the *Chao* decision."[144] Through these decisions the Court "cripple[d] the Act's core purpose of redressing and deterring violations of privacy interests."[145] Therefore, while Congress may have "established substantive duties in the Act that are expressly designed to prevent agency conduct resulting in intangible harms to the individual," the decisions have caused "a swath of Government violations to go unremedied."[146] At least one scholar claims members of Congress "believed that actual damages alone would be an inadequate remedy."[147] The House of Representatives even argued that the Act should include punitive damages.[148]

D. The OPM Breach and the Failure of the Privacy Act

Despite the potential of the Privacy Act to incentivize reasonable data security practices by agencies, the restrictive interpretation of "actual damages" has left victims of the OPM data breach without a remedy for the real emotional harms they have suffered.

OPM has admitted to the extensive scope of the data breach.[149] The background investigation records of millions of current, former, and prospective federal employees and contractors were stolen[150]—records that contained highly sensitive and personal data including fingerprints and employment, health, criminal, and financial history.[151]

---

142 *Id.* at 1453.

143 *Id.* at 1455.

144 Kardon, *supra* note 10, at 758.

145 *Cooper*, 132 S. Ct. at 1456 (Sotomayor, J., dissenting).

146 *Id.* at 1458–59.

147 Hong, *supra* note 83, at 89 (citing H.R. REP. NO. 93-1416, at 2–10 (1974)).

148 *Id.*

149 Cybersecurity Resource Center, *What Happened*, OPM.GOV (2015), https://www.opm.gov/cybersecurity/cybersecurity-incidents/#HowAmIAffected (noting the breach compromised sensitive information, including Social Security numbers, of 21.5 million individuals).

150 *Id.*

151 *Id.*

Additionally, the weaknesses in OPM's security were the result of a well-known accumulation of security breakdowns. In 2007, the U.S. Government Accountability Office identified significant weaknesses in federal information systems.[152] The report detailed how the implementation of access controls including passwords and encryption, which the agencies have not routinely implemented, could prevent data breaches.[153] OPM's Director, Katherine Archuleta, admitted that she was "aware of security vulnerabilities" and that simple protections such as encryption were not employed to protect the information affected by the breach.[154]

Despite facts that show violations of the Privacy Act that could be deemed willful, the current suits against OPM in response to the data breach struggle to show actual pecuniary harms resulting from an agency's failure to comply with the Privacy Act. Plaintiffs allege that they suffer "an increased risk of suffering from . . . loss" of the opportunity to control how their personally identifiable information is used; costs associated with prevention and detection of possible future identity theft; opportunity costs from attempting to mitigate consequences of the breach; and continued risk to their personal information.[155] Of all the alleged harms, only actual identity theft that the plaintiffs can directly link to the breach would qualify as "actual damage" under the Court's interpretation of the Act.[156]

In general, data breaches cause specific harms that create tremendous difficulties for plaintiffs, even before the narrowing of the Privacy Act's damages provision.[157] The (now familiar) warning notice, that informs its recipient that "[s]omeone may have taken possession of your credit-card info, Social Security number, bank account

---

[152] U.S. Gov't Accountability Office, Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk, GAO 07-935T, at 6–7 (June 7, 2007), http://www.gao.gov/cgi-bin/getrpt?-GAO-07-935T (listing a series of security breaches across federal agencies that "illustrate that a broad array of federal information and assets are at risk").

[153] *Id.* at 11–12.

[154] *OPM: Data Breach: Hearing Before the H. Comm. on Oversight and Gov't Reform*, 114th Cong. 14 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management).

[155] Class Action Complaint & Demand for Jury Trial at 37–39, Woo v. U.S. Office of Pers. Mgmt., C.A. No. 6:15-cv-01220-MLB-GEB (D. Kan. 2015).

[156] Additionally, it might be very difficult to prove a causal relationship between the OPM breach and any pecuniary losses resulting from identity theft. Kardon, *supra* note 10, at 758–59 ("The victim would have to either demonstrate that the government's misuse of information led to the information falling into the wrong hands or prove the negative fact that neither the victim nor anyone else with access to the relevant information ever put the information's security in jeopardy.").

[157] *Id.* (referencing the difficulties plaintiffs have in demonstrating "willfulness and intent").

or other personal data that would enable him or her to go on a permanent shopping spree," leaves the victim to deal with anguish and uncertainty.[158] The loss of personal information "commonly cause[s] fear, anxiety, or other emotional distress."[159] The loss and theft of millions of personal records primarily generates emotional trauma, causing stress and fear of future identity theft or credit difficulties, and despite the massive scale of the breach, "emotional distress is generally the only harm the claimant suffers . . . [if] the identify theft apprehended never materializes."[160] Based on the Supreme Court's interpretation of actual damages, the most common harms would not fit the Court's narrow definition of damages compensable under the Act.[161] As a result, "individuals can no longer recover what [Supreme Court] precedents and common sense understand to be the primary, and often only, damages sustained as a result of an invasion of privacy, namely mental or emotional distress."[162]

Moreover, while the "adverse effect" requirement includes any harm that is sufficient to confer Article III standing, it is unclear whether the kinds of harms generated from data breaches even rise to that level. There is currently disagreement among the courts of appeals regarding whether the injuries from data breaches, including credit monitoring and fear of identity theft, are sufficiently imminent to grant Article III standing.[163] This Note does not aim to resolve that issue, but rather suggests that, even under a generous interpretation, these harms, while sufficient for Article III standing, fall short of "actual damages" as the Court has defined them. The emotional damages—even when certain enough to satisfy the standing require-

158 Steven Levy et al., *Grand Theft Identity*, NEWSWEEK, July 3, 2005, at 38, 40.

159 Doe v. Chao, 540 U.S. 614, 634 (2004) (Ginsburg, J., dissenting); *see* Hong, *supra* note 83, at 107–08 (arguing that most victims suffer significant nonmonetary harms as a result of identity theft).

160 *Chao*, 540 U.S. at 634 (Ginsburg, J., dissenting).

161 *See* FAA v. Cooper, 132 S. Ct. 1441, 1451 n.7 (2012) (quoting WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS § 112, at 761 (4th ed.1971)) (describing nonrecoverable, nonpecuniary damages as those that "may be recovered for the injury to the plaintiff's reputation, his wounded feelings and humiliation, and resulting physical illness and pain, as well as estimated future damages of the same kind").

162 *Cooper*, 132 S. Ct. at 1456 (Sotomayor, J., dissenting).

163 *Compare* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) (holding that allegations by customers—whose credit card numbers were stolen during a cyberattack on a store's computer data system—that they sustained aggravation and the loss of the value of their time in changing their card numbers and monitoring their accounts was sufficient for Article III standing, since there was a reasonable likelihood that the customers would be subjected to future fraudulent charges and other injuries as a result of the data breach) *with* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (holding speculation regarding the future use of personal information to be hypothetical and insufficient to establish standing).

ment—are not compensable under the Privacy Act according to the holding in *Cooper*.[164] "Although many plaintiffs whose personal information is leaked by an agency suffer emotional distress, such emotional distress is not sufficient to constitute an actual loss for many courts."[165]

Even if some victims are able to show that they have suffered identity theft, the agency will not internalize the *full* cost of the data breach, and will be underdeterred from continuing inadequate data practices.[166] Individuals who have suffered identity theft often seek to mitigate the threat of future identity theft through the purchase of credit monitoring.[167] Yet, even if courts are willing to deem the impending harm of identity theft a "substantial risk that the harm will occur,"[168] the Court's definition of "actual damages" places a large hurdle to recover mitigation expenses incurred to prevent future harm.[169]

Thus, the Privacy Act significantly underdeters agencies from taking adequate security measures since the vast majority of data breach victims are left without a remedy under the Act, with the loss of their private information not considered to cause any "actual damages."

III
Reconsidering the Constitutional Right to Informational Privacy

The Supreme Court's narrow interpretation of the Privacy Act has consequences for its jurisprudence regarding the informational right to privacy because the Act's protections are considered when courts determine whether there was a constitutional violation. Even if the Supreme Court's application of the cannon of sovereign immunity and interpretation of the Privacy Act's damages provision reflects the

164 *See* discussion *supra* Section II.C.

165 Solove & Hoofnagle, *supra* note 20, at 380.

166 *See In re* Science Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (noting that, on average, only 19% of victims of data breaches ultimately suffer identity theft).

167 *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966–69 (S.D. Cal. 2014) (alleging expenses incurred to purchase credit monitoring services as a cognizable injury in the aftermath of a breach).

168 *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) (indicating that standing can be based on a "'substantial risk' that the harm will occur").

169 *See* Beaven v. U.S. Dep't of Justice, 622 F.3d 540, 557 (6th Cir. 2010) (declaring it unreasonable to take future protective measures where plaintiffs have not proved that the disclosure had caused adverse effects to date).

will of Congress,[170] this Part argues that the narrow definition of compensable damages alters the Court's balancing test in *NASA v. Nelson*, and examines the impact of holding the government liable for data breaches.[171]

The constraint on the Privacy Act's remedy for data breaches contravenes the Court's rationale in *Nelson* that the Act is sufficient to allay concerns about OPM's collection of personal information. The underdetterence that results from the restrictive interpretation of "actual damages" leaves the requirements imposed in the Act effectively unenforceable.[172] While the Act also provides for criminal penalties for certain violations by government employees,[173] "the range of activities that are criminally punishable is considerably narrower than the range of activities for which civil suit may be brought," making it even less of an incentive than the ineffective civil remedies provision.[174]

Section III.A suggests that the ineffectiveness of the Privacy Act opens the door for lawsuits alleging a constitutional violation where agencies fail to maintain adequate levels of data security. Then Section III.B addresses potential concerns with placing significant weight on civil liability when balancing the interests that implicate the constitutional right to informational privacy.

A. Holding the Government Liable

In the wake of data breaches, individuals can bring a suit alleging a constitutional violation of the right to informational privacy by agencies that collect personal data but fail to enact appropriate security measures.[175] If the balancing test determining the permissible scope of encroachment into the informational privacy right is recalibrated based on the restricted damages under the Privacy Act, then the con-

---

[170] *See* Fitzpatrick v. IRS, 665 F.2d 327, 330 (11th Cir. 1982) ("The evolution and structure of the damage provisions indicate Congressional intent to restrict damage liability to a maximum consistent with private enforcement of the Act. Throughout the Privacy Act debate, a central concern was the scope of potential government liability for damages."), *abrogated by* Doe v. Chao, 540 U.S. 614 (2004); Kardon, *supra* note 10, at 739 (arguing that Congress placed a number of hurdles in the way of liability).

[171] NASA v. Nelson, 562 U.S. 134, 147–48 (2011) (holding that a questionnaire asking employees about treatment or counseling for recent illegal drug use did not violate the right to informational privacy, assuming such a right is protected by the Constitution).

[172] Kardon, *supra* note 10, at 737 ("[T]he recovery of actual damages through civil suits is the primary mechanism for deterrence . . . .").

[173] 5 U.S.C. § 552a(i) (2012).

[174] Kardon, *supra* note 10, at 738.

[175] *See* Froomkin, *supra* note 114, at 1051–56 (describing how the constitutional right to informational privacy could be pleaded as a Section 1983 claim or a *Bivens* claim to recover damages from the government for the constitutional violation).

stitutional right could result in fuller remedies for injuries caused by accidental or illegal data breaches than the Act currently allows.[176]

The holding of *Nelson* no longer rests on firm ground.[177] The Privacy Act neither adequately protects individuals, by allowing them to recover for the injuries suffered when their data is stolen, nor incentivizes agencies to protect information from a breach.[178] The Act is intended to protect "important interests in information privacy, and even though knowledge of this purpose [has been] of limited use to courts interpreting the damage provisions, it should be a guiding force behind [reform]."[179] Agencies should face "[a] regulatory regime that requires costly breach notifications, or imposes actual fines, [and] creates an incentive to act in a manner that minimizes the expected total cost of prevention and cure."[180]

The Privacy Act's ineffectiveness can shift the balancing test used to determine the permissible scope of government conduct. Consider again the Third Circuit's enumerated balancing factors: the information disclosed, the potential for harm from nonconsensual disclosure, whether there is public interest militating toward access, and the *adequacy of safeguards* to prevent unauthorized disclosure.[181] In the case of the OPM breach, the potential for harm and the type of information accessed both weigh heavily in favor of the individuals, many of whom had their fingerprints and medical histories stolen.[182] Moreover, while there is a government interest in access,[183] the shift in the interpretation of the liability provision of the Privacy Act leaves the

176 *Id.*

177 *See supra* Part II. The Supreme Court has indicated that developments in the law that underlie past decisions are one of the prerequisites for overturning past decisions. *See* Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 855 (1992) (outlining the considerations for applying stare decisis). The *Nelson* ruling relied heavily on the assumption that the Privacy Act would provide adequate privacy protection partially through incentives for adequate data security. NASA v. Nelson, 562 U.S. 134, 156–57 (2011).

178 While the Privacy Act expressly requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained," civilians will be unable to enforce this section which attempts to prevent emotional and dignitary harms based on the ruling in *Cooper*. 5 U.S.C. § 552a(e)(10) (2012); *see also supra* Section II.C.

179 Kardon, *supra* note 10, at 767.

180 Froomkin, *supra* note 114, at 1035.

181 United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (listing factors courts should balance when defining the right to informational privacy).

182 *See supra* notes 1–5 and accompanying text (describing data stolen in the OPM breach).

183 *See supra* notes 42–44 and accompanying text (describing the government's interest in background checks).

safeguards inadequate, and may shift the balance and appropriateness of the government infringement.

Where the Privacy Act fails to ensure reasonable data security, the courts should adjust the balancing test and account for this fact. "[F]ailing to update software and leaving known exploits unpatched, placing private data in public files online, losing laptops, tapes, or USB drives with unencrypted (or weakly encrypted) data are all actions that make it easy for a third party to gain access to government-held data" and militate in favor of holding the government liable in the event of a breach.[184]

As scholars have argued, individuals would then be able to seek remedies outside the scope of the Privacy Act. Plaintiffs could pursue either a Section 1983 or *Bivens* claim for damages, or seek injunctive relief for the violation of a constitutional right.[185] Damages could provide incentives for agencies to maintain adequate security, while injunctive relief would prevent the agencies from gathering data until the agency took steps to improve data security.

B. Concerns with a Focus on Constitutional Liability

Despite this Note's contention that the restriction of the Privacy Act's damages provision should alter the balance of interests when confidential information is at issue, agency data security presents a number of difficulties that stand in the way of effective regulation through the judicial recognition of a constitutional right to informational privacy. Some may doubt the effectiveness of ex post money-damages liability, while others may worry that the scope of a constitutional right to privacy may be too broad and impose excessively punitive liability. This Subpart argues that while the complexities of agency regulation must be considered, liability under the Constitution will improve the governance of data security.

First, some scholars have argued that judicial review does not protect or appropriately recognize the value and importance of substantive rights.[186] These scholars argue that governments do not inter-

---

[184] Froomkin, *supra* note 114, at 1052. 42 U.S.C. § 1983 (2012) authorizes an action for damages (or other relief) against any "person" who, acting "under color of" state law, denies any federal right. *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971), creates an analogous cause of action against federal officials.

[185] *See* discussion *supra* note 184.

[186] *E.g.*, Daryl J. Levinson, *Making Government Pay: Markets, Politics, and the Allocation of Constitutional Costs*, 67 U. CHI. L. REV. 345, 350–51 (2000) (describing the disconnect between the monetary value courts place on rights and governments' ability to internalize those costs). Others have noted that many substantive rights are protected by other mechanisms than judicical review. *See* Joshua A. Rubin, Note, *Nonjudicial Fangs:*

nalize costs and thus will not be motivated to achieve an optimal level of constitutional compliance.[187] These individuals believe that agencies do not behave like private market participants.[188] The internalization of costs and benefits that is accepted as a rationale for imposing tort damage under the law and economics view of how private actors respond to incentives does not apply to government agencies. If agencies do not aim to maximize profits by minimizing the net costs of their actions, how will the imposition of additional liability motivate agencies to implement optimal data security?

Indeed, recognizing the distinctions between the government agencies and private firms that manage private data is essential to achieving adequate security across the board. Like private firms, many agencies have begun to acknowledge privacy concerns and have appointed privacy officers or created committees to provide privacy oversight.[189] Furthermore, there is no doubt that agency officials face political pressures and constrained budgets that can prevent the optimal internalization of civil liability. When the U.S. Treasury writes a check to make individuals whole for a constitutional violation, the only pressure OPM officials feel stems from congressional hearings, not reduced profits as if the agency was a private firm.

However, the additional protections and remedies will help focus the agencies' attention on the most serious threats, compensate individuals for serious violations of their rights, and strengthen private-data protections. Primarily, it is unwise to leave agencies in charge of policing their own data security,[190] a mandate with which they have

Defending the Privacy Act's Complete Civil Remedies Exemption, 90 N.Y.U. L. REV. 1409, 1429–31 (2015) (describing scholarship that argues against a court-centric approach to substantive legal norms).

187 *Levinson*, *supra* note 186, at 350.

188 *Id.*

189 Rubin, *supra* note 186, at 1437–40. For example, the IRS was an early mover through the creation of the Office of the Privacy Advocate. Margaret A. Irving, *Managing Information Privacy in the Information Age*, 53 ADMIN. L. REV. 659, 668–71 (2001). Rubin identifies the Department of Homeland Security's creation of the Chief Privacy Officer position as another method of ensuring agency actions and privacy commitments are examined. Rubin, *supra* note 186, at 1438–39.

190 There is a perceived conflict of interest in a scheme where an agency plays a role in policing its own behavior. *See, e.g.*, Fran Quigley, *Torture, Impunity, and the Need for Independent Prosecutorial Oversight of the Executive Branch*, 20 CORNELL J.L. & PUB. POL'Y 271, 273 (2010) (noting a "clear conflict of interest" that exists when the Attorney General—who serves at the pleasure of the President—is responsible for investigating the President or other top officials); *cf.* Caprice L. Roberts, *The Fox Guarding the Henhouse?: Recusal and the Procedural Void in the Court of Last Resort*, 57 RUTGERS L. REV. 107, 168 (2004) (describing and deeming problematic the process by which Justices decide for themselves whether they will be recused, and arguing that "[c]orrection of this flaw requires that other, non-implicated Justices participate in the decision-making process").

repeatedly failed to comply.[191] "Current oversight and enforcement efforts have been unsuccessful . . . . Federal agencies have been unwilling to police themselves."[192] The current model of nonjudicial enforcement of the Act has simply not resulted in adequate security. Additional liability can only help provide increased protections for individuals.

Moreover, this Note has argued that the *Cooper* decision altered the balance of interests at issue when the government collects private data. Correcting this balance does not require the imposition of damages, but rather—as in *Fraternal Order*[193]—courts will be able to exercise injunctive power that is lacking under the Privacy Act to prevent the collection of information until security is brought up to acceptable standards. Meanwhile, by imposing monetary damages, courts will be able to compel compensation akin to insurance for the violation of a constitutional right.[194] Combining the injunctive power with civil liability for violations of individuals' privacy serves to recognize the importance of individual privacy that the Court has found in the Constitution[195] and Congress attempted to defend in the Privacy Act.[196]

Furthermore, many of the differences between the federal government and private sector employers weigh in favor of stronger security requirements. Most personal data held by private companies "is generated incident to, or accompanied by, an economic transaction."[197] While the government-mandated background checks for employment are more consensual than the information collected by statutory mandate, they lack the key characteristics of private-data collection: that the data subject could have chosen to forgo the exchange, or could have instead chosen to transact with another company.[198]

Competition and choice are restricted in the government context. The existence of choice is key to private sector regulation and protection of consumer privacy.[199] While firms invest in data security from a

---

191 *See* Auerbach, *supra* note 3 (describing the repeated security failures that led to the OPM breach).

192 Coles, *supra* note 92, at 990.

193 Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia, 812 F.2d 105, 118 (3d Cir. 1987) (issuing an injunction preventing data collection until security was improved). *See also supra* notes 45–52 and accompanying text.

194 Levinson, *supra* note 187, at 404.

195 *Supra* Section I.A.

196 *Supra* Section II.B.

197 Froomkin, *supra* note 114, at 1024.

198 *Id.*

199 Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 815 (2011).

wealth-maximizing perspective,[200] the government does not have the same profit or reputational concerns to drive protections of privacy. Thus, the Privacy Act and constitutional restrictions serve as a necessary mitigating force, correcting the disparity between private and public incentives.

As an alternative, many scholars have suggested that Congress amend the Privacy Act.[201] However, the current absence of civil liability for data breaches exposes Congress's failure to pass legislation that will protect individual privacy rights.[202] While a Privacy Act amendment or additional legislation is not an impossible solution, recent congressional behavior suggests little interest in expanding the civil liability provision of the Act. Congress responded to both *Chao* and *Cooper* with inaction and silence—furthering the need for judicial action.

Additionally, opponents to constitutional liability may claim that the Privacy Act cannot prevent all breaches or third-party thefts of data and that additional liability may overdeter agencies from collecting important information or handcuff agencies who operate with limited budgets. The imposition of a balancing test on a wide range of government activities may create uncertainty detrimental to the functioning of the government.[203]

Regardless of the potential for "no fault" breaches even when the Privacy Act functions perfectly, the Privacy Act *as interpreted* currently falls short in its ability to protect individuals' privacy. It is true that the Court held that "[a]n ironclad disclosure bar" is not required to "satisfy privacy interests."[204] However, the Privacy Act is not merely less than ironclad, but is in fact completely impotent when it comes to protecting individual privacy.[205] The lack of recovery for emotional damages leaves agencies without a penalty for the failure to

---

[200] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 928 (2007) (noting that disclosure requirements provide incentives for private firms to increase data security).

[201] *See, e.g.*, Hong, *supra* note 83, at 109–11 ("Congress should increase the amount of recoverable damages."); Kardon, *supra* note 10, at 767 ("Congress should act accordingly by amending the language of the damages provision of the Privacy Act to clearly allow for recovery on the basis of nonpecuniary harms.").

[202] Coles, *supra* note 92, at 990 ("[T]he efforts of Congress . . . to provide guidance and to ensure compliance have met with limited success . . . . Ultimately, it is the flawed statutory enforcement and oversight scheme that is responsible for the failings of the Privacy Act.").

[203] *See* NASA v. Nelson, 562 U.S. 134, 167 (2011) (Scalia, J., concurring) (arguing that the Court's treatment of the right to informational privacy provides no guidance for lower courts due to "the sheer multiplicity of unweighted, relevant factors" courts can consider).

[204] *Nelson*, 562 U.S. at 157 (Alito, J., majority opinion).

[205] *Supra* Part II.

comply with a number of the Act's provisions. Moreover, where the Privacy Act *does* adequately regulate the maintenance of individuals' data, this Note does not argue that the balancing test should always favor liability. Instead, where the Court's narrow construction of "actual damages" in the Privacy Act generally leaves victims of a data breach without any injury under the Act *and* that result leaves agencies underincentivized from establishing appropriate data security to protect individuals' privacy should the balance of interests be affected.

The readjustment of the balancing test defining the permissible infringement into the alleged constitutional right to informational privacy could be an effective method of regulating government data security. The narrowing of the definition of "actual damages"[206] should be accounted for by courts conducting a balancing test of the individual privacy interests and the government's interest in collecting personal data.[207] If courts view the elimination of emotional harms from the "actual damages" section of the Privacy Act in *Cooper* as weighing in favor of more limited government infringement of private data, the right to privacy will serve to incentivize data security by federal agencies. Agencies will quickly learn the requirements of data security and adjust their practices as necessary.

Therefore, courts must recognize the importance and weight of "the adequacy of safeguards to prevent unauthorized disclosure"[208] as one of the central factors to ensuring the right to informational privacy is not violated. Where the Privacy Act originally intended to hold agencies liable for inadequate security[209] responsible, but breaches are now going unremedied,[210] a balancing test that recognizes the shift in the incentives for adequate security will fill the gaps that have developed in federal privacy protections and incentivize agencies to maintain a reasonable standard of security.

CONCLUSION

The data breach OPM suffered exposed the personal information of millions of Americans while revealing that the Supreme Court's decision in *Nelson* may no longer stand on firm ground. As the

206 *Supra* Section II.C.

207 *See In re* Crawford, 194 F.3d 954, 959 (9th Cir. 1999) ("[T]he right to informational privacy, however, is not absolute; rather it is a conditional right which may be infringed upon a showing of proper governmental interest.").

208 *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (defining "factors which should be considered in deciding whether an intrusion into an individual's privacy is justified").

209 *Supra* Section II.B.

210 *Supra* Section II.D.

increasingly narrow interpretation of the Privacy Act has left the victims without an ability to either receive compensation for their losses or hold OPM responsible for their reckless and inadequate protection of the data, courts must reexamine the definition and scope of the constitutional right to informational privacy. Given its proper weight, the inadequate security wrought by the Court's interpretation of the Act should shift the balance of interests—allowing individuals to sue the government for a violation of their Fourteenth Amendment right to informational privacy, thereby encouraging reasonable data security by federal agencies.