GOVERNMENT DATA BREACHES

By A. Michael Froomkin†

TABLE OF CONTENTS

I. INTRODUCTION

Private data held by the government is not the same as private data held by others. Much of the government's data is obtained through legally required disclosures or participation in licensing or benefit schemes where the government is, as a practical matter, the only game in town. These coercive

---

† University of Miami School of Law. Thanks are due to Caroline Bradley, Reid Cushman, and Patrick Gudridge for helpful conversations, as well as to Barbara Brandon, Kaema Akpan, Adam Schlosser and Victoria Wilson for research help.

or unbargained-for disclosures impute a heightened moral duty on the part of the government to exercise careful stewardship over private data. But the moral duty to safeguard the data and to deal fully and honestly with the consequences of failing to safeguard them is, at best, only partly reflected in state and federal laws and regulations.

Activists, academics, and state legislatures have identified and, in some cases, taken significant preliminary steps to address the problem of data breaches—the unintentional release of personally identifiable information by lawful holders of the data—in the United States.[1] To date, however, the primary focus of these efforts in the U.S. has been private data breaches.[2] This paper addresses a related problem that, while by no means ignored, has not received the attention it deserves: data breaches in the U.S. public sector.[3]

The problem of public data breaches is similar to that of private data breaches, but there are also major differences relating to the nature of the information, the means by which the information is collected, and especially the legal and institutional regime under which the information is held. For example, much government-held data is acquired via legal compulsion or the result of processes where there is neither competition nor bargained-for exchange. These and other differences make the public problem more heterogeneous and arguably less tractable than its private cousin. As a result, while both the prophylactic and corrective justice solutions to the public data breach problem have important resemblances to the solutions aimed at the private sector, the differences are also substantial.

I begin this paper with an illustrative survey of the ways in which government data and government data breaches resemble and differ from private data breaches. I also briefly survey the extent to which the government's moral duty to safeguard data is currently instantiated in statutes and, increasingly, in regulations. Because governments determine what defines an ac-

1. *E.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 380 (2006).

2. *E.g.*, ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY (2008) (advising firms and analysts to apply economic principles to breach problems); Stephen Schauder, *Developments in Banking and Financial Law: 2005*, 25 ANN. REV. BANKING & FIN. L. 109, 111-18 (2006) (discussing the difficulty in balancing the needs of consumer privacy, security, and costs in developing privacy regulation); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915-28 (2007) (discussing laws that require private companies to notify individuals of data security incidents involving their personal information).

3. Previous treatments of the government data breach problem include Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693, 725-26 (2007) (arguing against new regulation at present) and Solove & Hoofnagle, *supra* note 1, at 379-80 (noting gaps in the Federal Privacy Act).

tionable data breach and what remedies are available for damages caused by these breaches, it is not surprising that the remedies available to victims of a government data breach are often less than those available to victims of private sector data breaches.

Part III of this paper discusses the extent to which the government's duty to safeguard private data has a constitutional foundation. I argue that there is a constitutional right, either free-standing or based in Due Process, against government disclosure of personal data lawfully acquired under legal compulsion, at least in cases where the government failed to take reasonable precautions to safeguard the data. This right is separate from any informational privacy rights that constrain the government's ability to acquire personal or corporate information.

The argument requires at most a small, logical extension of existing law; arguably, existing law already encompasses it. The key, oddly enough, is Chief Justice Rhenquist's opinion in *DeShaney v. Winnebago County Department of Social Services*.[4] In the course of explaining why recovery was not appropriate in a child-abuse case where the government, although on notice, did nothing, the Chief Justice distinguished a class of cases in which the government would be liable: those cases where the government took such full control of the situation that it displaced, and disempowered, the relevant private parties. Although the Chief Justice's opinion contemplates people in totalizing institutional settings such as government-run prisons or asylums, it is, at most, a tiny stretch to apply his logic to data held by a government. In the case of government data breaches, the government has full control over the data before releasing it; there is nothing that the subject of the data can do to influence the conditions under which the data is secured.

When the government releases private information without a legal right to do so it harms the subject of the data. The harm is equally large, and should be equally compensable, whether the breach was intentional or negligent. Under the *DeShaney* logic, victims of many governmental privacy breaches should have a claim against states under 42 U.S.C. § 1983 (2006). Similar constitutional claims against the federal government would require a *Bivens* action[5]; I examine, but ultimately reject, a theory of government liability based directly on a *Bivens*-style constitutional privacy tort in light of the Supreme Court's current hostility to expansion of *Bivens*.[6] As a result, persons injured by federal data breaches will have substantially inferior remedies available to them than will victims of state breaches. Further, in both state

4. 489 U.S. 189 (1989).
5. *See* Bivens v. Six Unknown Fed. Narcotics Agents, 403 U.S. 388 (1971).
6. *See infra* Section III.B.2.

and federal cases, victims will find that claims for effective remedies may be hampered by governmental immunity and the problem of valuing the harms caused by a breach.

II. THE NATURE OF GOVERNMENT DATA BREACHES

In this Part, I survey the factual and legal background relating to government data breaches in the U.S. It begins with an introduction to the great quantity and variety of data held by federal and state governments, then looks at the limited statistics available regarding the types, frequency, and size of government data breaches. The final three sections consider three types of prophylactic responses: the legal regime governing breaches; the incentive structure in which the breaches occur; and the federal government's recent improvements in the federal regulatory data-holding regime—improvements that are notably silent as to the issue of compensation for breaches.

A. NATURE OF THE DATA

Governments hold a wide variety of data on natural and legal persons, great both in scope and in scale. Numerical comparisons with the private sector are difficult given the inherent difficulties of quantification and the lack of detailed information as to how much data both groups actually hold.[7] In addition, data held by the public and private sectors overlap due to data sharing and data transactions.[8] There is no doubt, however, that federal and state governments hold a wide variety of data about persons and firms (See Tables 1 & 2).

7. For example: does one count bytes, records, or persons in the system? The extent to which disparate decentralized record systems permit cross-referencing is also difficult to quantify. Governments have the greatest breadth of information, e.g. census records. Yet, businesses may in some cases have more fine-grained data if they capture, for example, the details of economic transactions and internet clicktrails. Choicepoint alone is said to have over nineteen billion "records" in its databases. *See* John T. Fakler, *ChoicePoint Settles with FTC*, S. FLA. BUS. J., Jan. 30, 2006, http://southflorida.biz-journals.com/southflorida/stories/2006/01/30/daily13.html. But without more information as to the nature of those records, gross comparisons to state and federal databases are unlikely to be very meaningful.

8. *See, e.g.*, Fred. H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 439 (2008).

Table 1: Illustrative Types of Federal Government Data

Census data[9]	Personal tax data[10]
Corporate tax data[11]	Military records[12]
National security intercepts (e.g. telephone/e-mail intercepts by NSA)	Law enforcement data (e.g. FBI investigative data)
Prison records[13]	Passport applications[14]
Health records (e.g. VA, Medical benefits programs)	Transfer program records (e.g. Social Security, Food Stamps, Veterans)
Federal employee records[15]	Regulatory disclosures (e.g. trade secrets, required disclosures, results of inspections)
Contracting, purchasing[16]	Sealed court records[17]
Immigration records	

9. *See, e.g.*, 13 U.S.C. § 8 (2006).

10. *See, e.g.*, 26 U.S.C. § 6107(b) (2006).

11. *See, e.g.*, INTERNAL REVENUE SERVICE, STATISTICS OF INCOME - 2006: CORPORATION INCOME TAX RETURNS (2006), *available at* http://www.irs.gov/pub/irs-soi/06coccr.pdf.

12. *See, e.g.*, 32 C.F.R. § 70.8(b)(9)(i) (2009).

13. *See, e.g.*, 28 C.F.R. § 512.15 (2009).

14. *See* U.S. Department of State, Obtain Copies of Passport Records, http://www.travel.state.gov/passport/services/copies/copies_872.html (last visited Oct. 12, 2009).

15. *See, e.g.*, 41 C.F.R. § 105-56.015(c) (2009).

16. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, INTERNATIONAL TRADE: CURRENT GOVERNMENT DATA PROVIDE LIMITED INSIGHT INTO OFFSHORING OF SERVICES, GAO 04-932, at 28-29 (2004), *available at* http://www.gao.gov/new.items/d04932.pdf

17. *See, e.g.*, 6 C.F.R. § 27.400(i)(4) (2009).

Table 2: Illustrative Types of State/Local Government Data[18]

State tax data[19]	State law enforcement data (e.g. police records)
K-12 & university educational records[20]	Records relating to foster children and other reported to child welfare agencies[21]
State transfer programs records	State court records (including, in particular, family court)
State prison records[22]	State regulatory data[23]
State contracting, purchasing	Personal, occupational, and corporate license data (e.g. Driver's Licenses, Bar membership, Contractor licensing)[24]
Records deposited in connection with Driver's License applications subject to the REAL ID Act[25]	

Most privately acquired data is generated incident to, or accompanied by, an economic transaction. Even private medical records originate in a transaction with an important economic component, such as the purchase of medical services or medicine. One characteristic shared by almost all private non-medical transactions is that the data subject could have chosen to forgo the exchange, or could have instead chosen to transact with another entity. Of course, alternatives may be less convenient or more expensive, but the choice nonetheless exists.

The most important exception to this general rule of data collection incident to economic exchange may be that private sector data holders can acquire information about people from the government,[26] or as agents for the government. And there are undoubtedly a number of exceptions to the vo-

18. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 15 (2004) (noting that U.S. federal agencies and departments maintain nearly 2000 databases with records relating to immigration, financial history, welfare, licensing, etc); STAFF OF H. COMM.ON GOV'T REFORM, 109TH CONG., AGENCY DATA BREACHES SINCE JANUARY 1, 2003 (2006), *available at* http://oversight.house.gov/documents/20061013145352-82231.pdf.

19. *See, e.g.*, CONN. GEN. STAT. ANN. § 12-120a (West 2008).

20. *See, e.g.*, FLA. STAT. ANN. § 1002.22 (West 2009); W. VA. CODE § 48-9-601 (2001).

21. *See, e.g.*, CAL. WELF. & INST. CODE § 16011 (West 2002).

22. *See, e.g.*, 730 ILL. COMP. STAT. ANN. 5/3-5-1 (West 2009).

23. *See, e.g.*, N.C. GEN. STAT. ANN. § 58-2-69 (West 2009).

24. *See, e.g.*, ALASKA STAT. § 28.05.061 (2009).

25. REAL ID Act of 2005, Pub. L. No. 109-13, div. B, 119 Stat. 231, 302 (2005).

26. *Cf.* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595-98 (2004) (describing ways in which the government can acquire information from private sector data holders).

luntary character of the transactions, such as emergency medical assistance and the provision of monopoly utility services (such as electricity or natural gas), for which there is only one provider and the option to do without is not realistic.[27] But these cases, while significant in their salience and in the sensitivity of the personal data they give rise to, are nonetheless a very small fraction of the sources of private data in private hands.

Government-held data differs from privately held data in one critical respect: Most of the data listed in Tables 1 and 2 are either disclosures that are required by law (e.g. tax returns, the census, law enforcement) or created in connection with an activity for which there is no realistic alternative source or supplier (e.g. licensing or benefits). Other than government-as-employer, most of the major listed categories of government activity that generate data are not meaningfully optional.

B. TYPES, CAUSES, AND FREQUENCY OF BREACHES

"A data breach occurs when there is a loss or theft of, or other unauthorized access to, data containing sensitive personal information that results in the potential compromise of the confidentiality or integrity of data."[28] Personal data generally includes information that can be used to locate or identify an individual: name, address, telephone number, Social Security Number, driver's license number, account number, or credit or debit card number. It also includes more sensitive information, such as income, personal health records, military records, law enforcement investigatory records, and multifarious disclosures made in connection with the application for government licenses or benefits.

In addition to personal data, the government also maintains extensive records regarding corporations, partnerships, unions and other legal persons. These data include tax records, information submitted in connection with bids for government contracts, and often-voluminous submissions in connection with license applications. Firms in certain highly regulated industries, such as financial service providers, must also make regular detailed submissions in order to comply with their legal obligations.

1. Types and Causes of Breaches

While the data held by state and federal governments may be broader in scope than that held in the private sector, the types of data breaches to which

27. It may be notable that in many of these cases, the lack of choice arises out of or in connection with a government-granted monopoly.

28. Gina Stevens, *Federal Information Security and Data Breach Notification Laws*, CONG. RESEARCH SERV. REPORT RL34120 1 (2009), *available at* http://assets.opencrs.com/rpts/RL34120_20090129.pdf.

the data are vulnerable are in many cases similar. But while the public sector is vulnerable to all the risks that bedevil the private sector, there are some additional dangers that are either peculiar to the public sector or so different in scale as to amount to a difference in kind.

Government data breaches include both scenarios common to the private sector and some that are rarely found there (see Table 3).

Table 3: Major Types of Government Data Breaches

Data released intentionally, but in violation of law or regulations	Data released accidentally due to human error or misconfigured software
Data on physical media that is lost or stolen or otherwise not secured	Insider access in excess of defined permissions or for private purposes, or both
Malfunctioning or wrongly designed software[29]	Outside hackers,[30] viruses, trojan horses
Purportedly anonymized data releases that can be reverse engineered to create personally identifiable data (not unknown in the private sector, but of particular concern relating to census data)[31]	Foreign spying (contrast to industrial espionage in the private sector)

The Privacy Rights Clearinghouse attributed government data breaches in 2006 to five causes: "human/software incompetence" was the largest single cause, responsible for 44% of the cases found; laptop theft was second, accounting for 21%, with other thefts close behind at 17%; outside hackers caused 13% of the known cases; and insider malfeasance was blamed only 5% of the time.[32]

2. Frequency and Size of Breaches

At present, there is no unified and mandatory reporting system for state or federal data breaches. Thus estimates of the size and frequency of gov-

29. *See, e.g.*, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, THE INTERNAL REVENUE SERVICE DEPLOYED TWO OF ITS MOST IMPORTANT MODERNIZED SYSTEMS WITH KNOWN SECURITY VULNERABILITIES, 2008-20-163, at 2 (Sept. 24, 2008), *available at* http://www.treas.gov/tigta/auditreports/2008reports/200820163fr.pdf.

30. Hacking/breaking into a non-public government computer can result in fines or prison sentences ranging from one to twenty years depending on the severity of the breach. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

31. *See, e.g.*, LaTanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality,* 25 J.L. MED. & ETHICS 98, 100 (1997) ("In deidentified data, all explicit identifiers . . . are removed, generalized or replaced with a made-up alternative. Deidentifying data does not guarantee that the result is anonymous."); Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TECH CRUNCH, Aug. 6, 2006, http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/.

32. PRIVACY RIGHTS CLEARING HOUSE, CHRONOLOGY OF DATA BREACHES 2006: ANALYSIS (2007), http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm.

ernment data breaches rely to some extent on anecdote and guesswork. Nevertheless, even without comprehensive data there is no doubt that breaches of government data are frequent and significant. One recent commentator estimates that from 2000 to 2008, about 530 million records containing personal data were exposed or mishandled.[33] Of those incidents, 23% are estimated to be due to non-education government sources, with an additional 23% shared between public and private educational institutions.[34] Thus, the public sector accounted for somewhere between a quarter and half of all *reported* U.S. data breaches. When one considers that governments frequently are not covered by the increasing number of state data breach reporting statutes that reach private actors, it is possible that the true fraction is higher still.[35]

The Identity Theft Resource Center (ITRC), a private, non-profit group funded in part by data-brokers,[36] identified 110 breaches of state (excluding educational and health sectors), federal, and military databases in 2008, exposing 2,954,373 records.[37] In comparison, the ITRC documented 110 breaches of state and federal databases in 2007, exposing 8,156,682 records.[38] Since 2003, nineteen federal bodies have reported at least one loss of personal data that could potentially expose individuals to identity theft.[39] In one recent incident, the Department of Veteran's Affairs (VA) exposed the records of 26.5 million veterans and active-duty military personnel when computer

33. Jay Cline, *530M Records Exposed, and Counting*, COMPUTER WORLD, Sept. 9, 2008, *available at* http://www.computerworld.com/s/article/9114176/530M_records_exposed_and_counting.

34. *Id.*

35. On the other hand, according to IDENTITY THEFT RESOURCE CENTER, SECURITY BREACHES 2008 (2009), *available at* http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml, "[t]he Government/Military category has dropped nearly fifty percent since 2006, moving from the highest number of breaches to the third highest." To what extent this is due to improved practices, and to what extent this is an artifact of reporting rates is not clear.

36. IDENTITY THEFT RESOURCE CENTER, CORPORATE OVERVIEW 3 (2009), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Corp._Overview_200906 25.pdf.

37. IDENTITY THEFT RESOURCE CENTER, 2008 DATA BREACH STATS 19 (2009), *available at* http://www.idtheftcenter.org/BreachPDF/ITRC_Breach_Stats_Report_2008_final.pdf.

38. IDENTITY THEFT RESOURCE CENTER, 2007 DATA BREACH STATS 13 (2008), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_20071231_1.pdf.

39. *See* COMM. ON GOV'T REFORM, *supra* note 18, at 3-14 (listing the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, as well as the Office of Personnel Management and the Social Security Administration).

equipment was stolen from a VA employee's home.[40] Likewise, state breaches also occur. In 2008, for example, the Des Moines Register discovered that, since January 2005, the Iowa County land recorders had been posting documents containing the Social Security Numbers of thousands of Iowa residents, including the Governor, on a publicly available web site.[41]

C. UNIQUE LEGAL REGIME

Governments operate in a unique legal regime because they can define the legal definition of a data breach. Governments consider hacking—breaking into a non-public government computer—a serious crime that can result in fines or prison sentences ranging from one to twenty years depending on the severity of the breach.[42] Equally important, in the civil context, governments get to set the legal definition of what is a data breach and what is business as usual. Only some of the forty-four states with data breach statutes subject themselves to notice obligations similar to those that they impose on the private sector. In other words, subject only to federalism constraints and constitutional limitations, governments define which of their acts in releasing data constitutes an action for which the subject of the data can sue the government, just as they define the legal penalties for private data breaches.

State and federal governments also enjoy sovereign immunity. This immunity, however, is far from absolute because it does not protect state or federal governments from some constitutional claims.[43] Furthermore, both the federal and state governments have voluntarily abrogated their sovereign immunity for large classes of cases,[44] but even here there are limits. In addi-

---

40. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: AGENCIES REPORT PROGRESS, BUT SENSITIVE DATA REMAIN AT RISK, GAO 07-935T, at 6 (June 7, 2007), *available at* http://www.gao.gov/cgi-bin/getrpt?-GAO-07-935T.

41. *See* Jaikumar Vijayan, *Social Security Numbers Exposed on Iowa Land-Records Web Site*, COMPUTER WORLD, Sept. 5, 2008, *available at* http://www.computerworld.com/s/article/9114172/Social_Security_numbers_exposed_on_Iowa_land_records_Web_site.

42. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(3) (2006).

43. *See* James E. Pfander, *Sovereign Immunity and the Right to Petition: Toward a First Amendment Right to Pursue Judicial Claims Against the Government*, 91 NW. U. L. REV. 899, 972 (1997) ("[W]here the Constitution requires the government . . . to make victims . . . of constitutional violations whole, remedial obligations apply whether or not the government has adopted an effective waiver of sovereign immunity."); *see generally* Richard H. Seamon, *The Asymmetry of State Sovereign Immunity*, 76 WASH. L. REV. 1067, 1072-1102 (2001) (discussing current doctrines of state sovereign immunity); Gregory C. Sisk, *The Continuing Drift of Federal Sovereign Immunity Jurisprudence*, 50 WM. & MARY L. REV. 517, 574-87 (2008) (examining recent federal sovereign immunity jurisprudence). However, the Constitution imposes some limits on the power of the federal government to subject state governments to suit. U.S. CONST. amend. XI.

44. *See, e.g.*, Clark v. Barnard, 108 U.S. 436, 447 (1883) ("The immunity from suit be-

tion, through section 1983, the federal government has created a mechanism for citizens to sue states if their rights are violated.[45]

The leading example is *Collier v. Dickinson*, a rare, perhaps unique, data-privacy-related section 1983 claim decided in the Eleventh Circuit.[46] Executive-level officers of the Florida Department of Highway Safety and Motor Vehicles (DHSMV) were sued for selling personal information of plaintiffs to mass marketers in violation of the Driver Privacy Protection Act (DPPA).[47] The District Court originally dismissed the claim, holding that qualified immunity shielded the executives' actions.[48] The District Court also held that there is no constitutional right to privacy of the information provided to the DHSMV.[49] The Eleventh Circuit, however, held that the DPPA establishes a statutory right to privacy and that the plaintiff's allegation that the executives acted intentionally and willfully in violation of the DPPA survived summary judgment.[50] Rather than lose the suit, the government agreed to settle with the class of Florida drivers for $10.4 million, meaning that individual members of the class got $1—yes, a whole dollar—each.[51]

The fact that they have lawmaking power means that federal and state governments retain a unique ability to use their legislative, regulatory, and judicial power to define what constitutes a legal data dissemination and what liability they will bear for data breaches. Of those states that have breach laws covering the private sector, several impose duties on themselves similar to

---

longing to a State, which is respected and protected by the Constitution within the limits of the judicial power of the United States, is a personal privilege which it may waive at pleasure."). *But see* Seminole Tribe v. Florida, 517 U.S. 44, 59 (1996) (finding Congress does not have the power to abrogate state sovereign immunity unless it invokes Section 5 of the Fourteenth Amendment or the Interstate Commerce Clause).

45. Section 1983 creates a federal cause of action:

> Every person who, under color of any statute, ordinance, regulation, custom or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.

42 U.S.C. § 1983 (2006).

46. 477 F.3d 1306 (11th Cir. 2007).

47. *Id.* at 1307.

48. *Id.*

49. Collier v. Dickinson, No. 04-21351-CIV, 2006 WL 4998653, at *10 (S.D. Fla. Mar. 30, 2006) (citing Pryor v. Reno, 171 F.3d 1281, 1288 n. 10 (11th Cir. 1999)), *rev'd* 477 F.3d 1306 (11th Cir. 2007).

50. *Dickinson*, 477 F.3d at 1309-10.

51. Posting of Steve Bousquet to The Buzz: Florida Politics, *For Motorists, a Long Overdue $1 Credit*, http://blogs.tampabay.com/buzz/2009/01/for-motorists-a.html (Jan. 15, 2009, 14:53 EST).

those that they impose on the private sector,[52] but others do not.[53] A few states do provide for fines if the government fails to notify the victim and damages occur as a result of that failure.[54] Uniquely, Oklahoma has a breach law for the public sector, but none for the private sector.[55]

There is no logical reason why various types of unplanned data releases should trigger duties and sanctions when performed by private entities, but trigger no legal consequences when performed by governments. The arguments regarding planned, or permitted, data releases are more complicated. There are public policy reasons why some government disclosures should be encouraged, even if analogous disclosures by private parties might not be permitted. Yet the argument is not equally persuasive in all cases. On the one hand, some government disclosures clearly serve values of transparency,

52. *See* ALASKA STAT. § 45.48.010 et seq. (2009); ARIZ. REV. STAT. ANN. § 44-7501 (2008); ARK. CODE ANN. § 4-110-103 (West 2008); CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2009); DEL. CODE ANN. tit. 6, § 12B-102 (2008); HAW. REV. STAT. ANN. § 487N-2 (LexisNexis 2008); IDAHO CODE ANN. § 28-51-105 (2008); 815 ILL. COMP. STATE. ANN. 530/12 (LexisNexis 2009); IOWA CODE ANN. §§ 715C.1-715C.2 (West 2008); KAN. STAT. ANN. § 50-7a02 (2008); LA. REV. STAT. ANN. § 51:3074 (2008); MASS. GEN. LAWS ANN. ch. 93H, § 3 (West 2007); MICH. COMP. LAWS ANN. § 445.72 (West 2008); NEB. REV. STAT. ANN. § 87-802 (LexisNexis 2009); NEV. REV. STAT. ANN. § 603A.220 (LexisNexis 2009); N.H. REV. STAT. ANN. § 359-C:19 et seq. (2009); N.J. STAT. ANN. § 56:8-163 (West 2009); N.Y. GEN. BUS. § 899-aa, N.Y. STATE TECH. § 208 (2009); OHIO REV. CODE ANN. §§ 1349.19, 1347.12 (West 2009); S.B. 583, 74th LEGIS. ASSEMB., REG. SESS. (Or. 2007); 73 PA. STAT. ANN. § 2303 (West 2008); R.I. GEN. LAWS § 11-49.2-3 (2009); S.C. CODE ANN. §§ 39-1-90, 1-11-490 (2008); TENN. CODE ANN. § 47-18-2107 (2008); VT. STAT. ANN. tit. 9, § 2430 (2008) (excluding law enforcement agencies and the department of public safety); VA. CODE ANN. § 18.2-186.6 (West 2008); WASH. REV. CODE ANN. §§ 19.255.010, 42.56.590 (West 2009); W. Va. CODE ANN. § 46A-2A-101 (West 2009); WIS. STAT. ANN. § 134.98 (West 2009).

53. *See* COLO. REV. STAT. § 6-1-716 (2008); CONN. GEN. STAT. ANN. § 36a-701b (West 2009); D.C. CODE 28-3852 (2009); FLA. STAT. ANN. § 817.5681 (West 2008) (imposing duty on government only when data storage function was contracted out to private firm); GA. CODE ANN. § 10-1-911 (West 2008) (excluding government agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes); IND. CODE ANN. § 24-4.9-1-1 et seq. (West 2009); ME. REV. STAT. ANN. tit. 10, § 1348 (2008) (imposing duties only on information brokers and other persons); MD. CODE ANN., COM. LAW § 14-3504 (West 2008); MONT. CODE ANN. § 30-14-1704 (2007); N.C. GEN. STAT. ANN. § 75-66 (2009) (imposing a duty on the government only when a person knowingly publicizes the personal information of another with actual knowledge that the person whose personal information is disclosed has previously objected to any such disclosure); N.D. CENT. CODE, § 51-30-02 (2008); TEX. BUS. & COM. CODE ANN. § 521.053 (Vernon 2009); UTAH CODE ANN. § 13-44-202 (2008); WYO. STAT. ANN. § 40-12-502 (2009).

54. For example, Louisiana and New Hampshire award actual damages that result from failure to notify. LA. REV. STAT. ANN. § 51:3075 (2009); N.H. REV. STAT. ANN. § 359-C:21 (2007). On the other hand, Utah explicitly excludes these claims. UTAH CODE ANN. § 13-44-301(2)(a) (2008) ("Nothing in this chapter creates a private right of action.").

55. OKLA. STAT. ANN. tit. 74, § 3113.1 (West 2009).

which justifies rules such as the Freedom of Information Act (FOIA).[56] On the other hand, too much transparency may amount to little more than state-mandated data breaches when private information is posted online,[57] or if businesses' trade secrets, submitted in confidence as part of a regulatory proceeding, are released to the public.[58]

Governments, like firms, have a need for revenue, but only governments can legalize their own data breaches. Even here, however, federalism imposes limits, as demonstrated by Congress's reaction to the decision by some states to sell personal data collected incident to the issuance of driver's licenses. Congress enacted the Driver's Privacy Protection Act of 1994 (DPPA),[59] in order to regulate the disclosure of such information.[60] The DPPA's regulatory scheme restricts the State's ability to disclose a driver's personal data without the driver's consent,[61] and to reuse covered information acquired by private parties.[62]

The Supreme Court upheld the constitutionality of the DPPA in *Reno v. Condon*, rejecting a federalism challenge brought by South Carolina.[63] The lynchpin of Chief Justice Rhenquist's opinion is that the DPPA is similar to the statute upheld in *South Carolina v. Baker*, which was found to be constitu-

---

56. 5 U.S.C. § 552 (2006).

57. *See, e.g*, Vijayan, *supra* note 41.

58. Consider the facts of *Chrysler Corp. v. Brown*, sometimes called a "reverse FOIA case," in which Chrysler attempted to block the Defense Logistics Agency's release of its trade secret. 441 U.S. 281, 285, 291 (1979). The Supreme Court assumed that FOIA Exemption 4, 5 U.S.C. § 552(b)(4), would allow the agency to block release if it chose to do so. 441 U.S. at 285, 291. But the agency chose not to invoke Exception 4 and informed Chrysler of their intention to release the information. *Id.* at 287-88. The Supreme Court held that FOIA did not give Chrysler reason to object to the release, but remanded for consideration of the protections that might be available under the Trade Secrets Act, 18 U.S.C. § 1905. *Id.* at 318-19. The discretionary nature of the information release is illustrated by agency practices after *Chrysler*: in order to assure firms that agencies will not use their discretion to release information that the firms prefer to keep private, a category that extends well beyond trade secrets, agencies and firms enter into enforceable confidentiality agreements. *See, e.g.*, JEROME G. SNIDER, CORPORATE PRIVILEGES AND CONFIDENTIAL INFORMATION 2-77 (1999).

59. 18 U.S.C. §§ 2721-2725 (2006).

60. 138 Cong. Rec. H1785-01 (1992).

61. Note especially § 2721, which, with some exceptions, makes it an offense for a state department of motor vehicles officer, employee, or contractor to release personal data gathered in connection with a motor vehicle record, defined as a "motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." 18 U.S.C. §§ 2721, 2725 (2006). Permitted uses include safety recalls, law enforcement, civil and criminal proceedings and "use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license" required by law. 18 U.S.C. § 2721(b) (2006).

62. *See* 18 U.S.C. § 2721(c) (2006).

63. 528 U.S. 141, 143 (2000).

tional because it "'regulate[d] state activities,' rather than 'seek[ing] to control or influence the manner in which States regulate private parties.'"[64] Instead, "[t]he DPPA regulates the States as the owners of data bases,"[65] suggesting that the data are just another form of property subject to ordinary regulation.

Indeed, there are a few significant federal statutory and regulatory limitations on the ability of both state and federal governments to release private data at will. One of the most broad-reaching rules is the 1996 Health Insurance Portability and Accountability Act (HIPAA).[66] HIPAA applies to federal, state, and local government hospitals, as these meet the definition of a covered "health care provider."[67] HIPAA also applies to government health plans including the federal health care program for active duty military personnel and veterans.[68] Furthermore, HIPAA covers health care "clearinghouses" (processors of data created by another).[69] All entities subject to HIPAA must comply with complex, but somewhat toothless, regulations restricting the dissemination of electronically stored patient medical information.[70]

A recent amendment to HIPAA greatly increases the public consequences of a data breach by requiring that all health information breaches, including those by government health providers, be publicized if they involve more than 500 people.[71] The statute also directs the Secretary of Health and Human Services to maintain a website listing the firms responsible.[72] This represents a substantial change from the original HIPAA regime where covered entities had no duty to notify patients of breaches, but only to mitigate the harm.[73]

---

64. *Id.* at 150 (quoting South Carolina v. Baker, 485 U.S. 505, 514-15 (1988)).

65. *Id.* at 151.

66. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, § 261, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.).

67. *See* 42 U.S.C. § 1320d(3) (2006); 45 C.F.R. § 160.103 (2006).

68. *See* COVERED ENTITY CHARTS, HIPAA GENERAL INFORMATION 10, http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf. *But see* 45 C.F.R. § 164.512(k) (2009) (exemption for information uses or disclosures about members of the armed forces where "deemed necessary by military command authorities").

69. *See* 45 C.F.R. § 160.103 (2006) (defining a covered entity).

70. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. pts. 160 & 164 (2007).

71. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 13402, 123 Stat 115 (2009) (codified as amended at 42 U.S.C. § 17932 (2009)).

72. *Id.* at § 13402(e)(4).

73. *See* 42 U.S.C. §§ 1320d-1320d-8 (2006). *Cf.* Brandon Faulkner, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1116 (2007) (noting that pre-amendment "HIPAA does not require entities to notify individuals after unauthorized or wrongful disclosure of individually identifiable health information"); Nicolas P. Terry & Leslie P. Francis, *Ensur-*

There are also some laws specific to the federal government that do not apply to the states. Chief among the federal laws is the much-maligned Privacy Act of 1974,[74] (Privacy Act), which regulates the collection, maintenance, use, and dissemination of an individual's personal data by federal government agencies.[75] The Privacy Act requires:

> Each agency that maintains a system of records shall . . . 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.[76]

Critically, the Privacy Act creates a private right of action in federal district court whenever 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."[77] A successful Privacy Act claim requires (1) that the information be a record contained in a system of records, (2) that it have been disclosed improperly, willfully and intentionally, and (3) that the disclosure has caused actual damages.[78]

---

ing the Privacy and Confidentiality of Electronic Health Records, 2007 U. ILL. L. REV. 681, 729 (2007) (noting that pre-amendment "HIPAA seems too weak; it requires simply that custodians of electronic health information keep records about access that patients can review on request. The difficulty is that patients may not know that their records have been accessed and thus may not request information about access.").

74. 5 U.S.C. § 552a (2006). For critique, see for example, Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1088, 1114 (2002), arguing that federal statutory protections have "fared poorly in cases involving information privacy on the Internet." *See also* Jonathan C. Bond, Note, *Defining Disclosure In A Digital Age: Updating The Privacy Act For The Twenty-First Century*, 76 GEO. WASH. L. REV. 1232, 1258-64 (2008) (proposing some interesting suggestions as to how to modernize the Privacy Act); Dennis J. McMahon, Comment, *The Future Of Privacy In A Unified National Health Information Infrastructure*, 38 SETON HALL L. REV. 787, 797 (2008) ("Perhaps the most glaring loophole in the Privacy Act is the 'Routine Use' exception. This exception allows federal agencies to disclose personal information if they determine that the disclosure is part of the routine use of information and it is compatible with the original purpose for collecting the information.").

75. In addition, the E-Government Act of 2002, 44 U.S.C. § 3501 (2006), requires agencies to prepare privacy impact statements before creating new searchable databases or collecting new types of personally identifiable information. *See also* OFFICE OF MGMT. & BUDGET, PUBL'N NO. M-03-22, GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E-GOVERNMENT ACT OF 2002, (2003), *available at* http://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html.

76. 5 U.S.C. § 552a(e)(10) (2006).

77. *Id.* § 552a(g)(1)(D).

78. *See* Doe v. Chao, 540 U.S. 614, 619-21 (2004) (interpreting 5 U.S.C. § 522a(g)(4)(A) (2006)).

The Privacy Act has some teeth, but not too many, when applied to government data breaches. The leading case is *Doe v. Chao*.[79] Doe sued the Department of Labor (DoL) for illegal disclosure of his Social Security Number (SSN), which he had voluntarily disclosed on a benefits application.[80] The DoL then distributed documents to third parties that identified Doe by his SSN.[81] Doe filed suit under the Privacy Act, relying on the civil remedy section of the statute, which reads:

> In any suit . . . in which the court determines the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual an amount equal to the sum of actual damages sustained by an individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000.[82]

Doe argued this meant he was entitled to at least $1,000 if he proved a Privacy Act violation.[83] The government replied that Doe needed to prove actual damages before recovery, and the Supreme Court, in an opinion by Justice Souter, agreed that a showing of "actual damages" was required for recovery.[84] The opinion left the definition of "actual damages" for another day.[85]

The Privacy Act applies to intentional disclosures by the government. It has yet to be successfully invoked to award damages when records were hacked or forcibly accessed, although the recent decision in *American Federation of Government Employees v. Hawley* shows how this might change.[86] *Hawley* concerned the theft of a laptop hard drive containing personnel data for 100,000 Transportation Security Administration (TSA) employees, including SSNs, birth dates, payroll information, bank account numbers, and routing numbers.[87] The court explicitly addressed the issue of whether the government's actions amounted to intentional and willful conduct.[88] Given that the plaintiffs alleged that the TSA had been repeatedly warned about fundamental deficiencies in its security, the court ruled that there was sufficient evidence to suggest that the TSA knew of the risk of a data breach, but inten-

79. *Id.*
80. *Id.* at 616-17.
81. *Id.* at 617.
82. *Id.* at 619 (citing 5 U.S.C. § 552a(g)(4) (2006)).
83. *Id.* at 620.
84. *See id.* at 627.
85. *See id.* at 627 n.12.
86. 543 F. Supp. 2d 44 (D.D.C. 2008).
87. *Id.* at 45.
88. *Id.* at 51-52.

tionally and willfully ignored it, which sufficed for plaintiffs to survive summary judgment.[89] Thus, the District Court held that TSA employees, alleging that the agency had negligently lost control of their personal data by failing to establish safeguards to prevent the loss of hard drives, could state a claim for "embarrassment, inconvenience, mental distress, concern for identity theft, concern for damage to credit report, concern for damage to financial suitability requirements in employment, and future substantial financial harm, [and] mental distress due to the possibility of security breach at airports."[90] Central to this holding was the District of Columbia Circuit rule that emotional trauma alone suffices to state a claim of an "adverse effect" under section 552a(g)(1)(D) of the Privacy Act.[91] Even so, the trial court in *Hawley* noted that whether such injuries qualified as "actual damages," under the standard set in *Doe v. Chao*, remained uncertain.[92]

This preliminary ruling was enough to motivate the TSA to settle the plaintiffs' claim for twenty million dollars,[93] which means that no ruling on the merits of the Privacy Act claims arising from unintentional record disclosure will be forthcoming. And thus the definition of what amounts to "actual damages" under the Privacy Act remains unsettled.

D. DIFFERENT INCENTIVE STRUCTURE

The legal regime regulating government breaches matters because there is some reason to suspect that economic incentives work less well in the public sector than they do in the private sector. Economic theory suggests that firms should respond to financial carrots and sticks. A regulatory regime that requires costly breach notifications, or imposes actual fines, creates an incentive to act in a manner that minimizes the expected total cost of prevention and cure.[94] Firms are also presumed to be sensitive to secondary effects that might reduce their profits, such as bad publicity. State laws requiring breach notices rely on both of these tendencies for their effectiveness: Firms will find that providing the notices costs money and creates bad publicity. Lawsuits, or measures designed to preempt lawsuits, e.g. by offering discount

89. *Id.*

90. *Id.* at 50-51.

91. *Id.* at 51 n.12 (citing Krieger v. U.S. Dep't of Justice, 529 F. Supp. 2d 29, 53 (D.D.C. 2008) (quoting Albright v. United States, 732 F.2d 181, 186 (D.C. Cir. 1984)).

92. *Id.* at 53 (citing Doe v. Chao, 540 U.S. 614, 624-25 (2004)). *Cf.* Jacobs v. Nat'l Drug Intelligence Ctr., 548 F. 3d 375, 377 (5th Cir. 2008) (noting trend towards allowing emotional injuries to qualify as "actual damage" under Privacy Act).

93. 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.

94. For an attempt to put this into practice, see SHOSTACK & STEWART, *supra* note 2.

coupons or free credit monitoring, and responding to customer concerns and complaints, costs more still. It is arguable whether the people in firms who make decisions about information technology (IT) practices have a sufficient financial incentive via stock options or bonuses to be directly concerned about a breach's effect on the company's stock price or profitability, but it is possible that their bosses might. And in any case, being responsible for a well-publicized data breach disaster cannot be career-enhancing.

In contrast, governments and government employees are not especially sensitive to the profit motive. Many civil servants enjoy substantial security of tenure. They shelter not just behind the government's sovereign immunity, but also qualified immunity for many job-related tasks.[95] Government employees are rarely eligible for much in the way of bonuses, although their promotion prospects may be affected by their performance.[96] Economic theory suggests that financial incentives applied to the government organization—be they fines or a requirement to spend money on mitigation—are far less likely to be transmitted to the employee level. Remedies that might be more likely to work, such as dismissing persons whose negligence causes a data breach, are somewhat Draconian, and not obviously effective either.[97] On the other hand, given how easy it has become to encrypt sensitive data, leaving sensitive data unencrypted and then losing control of it may amount to the sort of gross negligence that deserves a strong remedy.

Even if graduated economic incentives are not likely to be very potent, there are other incentives that are more likely to be effective: civil servants and the very large majority of their elected political superiors are acutely sensitive to bad publicity. And news of data breaches, especially those resulting

95. Herring v. Keenan, 218 F.3d 1171, 1178-81 (10th Cir. 2000) (holding that qualified immunity barred otherwise valid *Bivens* action against probation officer as constitutionally based information privacy right against disclosure of HIV status to relatives was not clearly established at time disclosure was made); Helen L. Gilbert, Comment, *Minors' Constitutional Right to Informational Privacy*, 74 U. CHI. L. REV. 1375, 1385 (2007) (stating that "[Q]ualified immunity frequently bars damage awards for plaintiffs because of the ambiguous scope of informational privacy protections.").

96. *See* STEWARD LIFF, MANAGING GOVERNMENT EMPLOYEES 100, 124-25 (2007); PAUL C. LIGHT, A GOVERNMENT ILL EXECUTED: THE DECLINE OF THE FEDERAL SERVICE AND HOW TO REVERSE IT 226, 234 (2008) (noting the unusual nature of Departments of Defense and Homeland Security pay-for-performance system).

97. The UK government has a history of firing officials responsible for leaving secret documents on trains and taxis, but this zero-tolerance policy has not proved particularly effective. *See*, *e.g.*, *Intelligence Official Suspended over al-Qaeda File Left on Train*, TIMES (UK), June 12, 2008, http://www.timesonline.co.uk/tol/news/uk/article 4115588.ece; *More Secret Government Documents Left on Train*, DAILY TELEGRAPH, June 14, 2008, http://www.telegraph.co.uk/news/uknews/2131236/More-secret-government-documents-left-on-train.html; *Second Spy Loses Laptop*, THE REGISTER, March 28, 2000, http://www.theregister.co.uk/2000/03/28/second_spy_loses_laptop/.

from some form of negligence, make for extremely bad publicity.

E. FEDERAL BEST PRACTICES (STATE PATCHWORK)

As governments make the rules to which they themselves are subject, it can be difficult to institutionalize regimes that require governments to create bad publicity for themselves. But, as demonstrated by the HIPAA amendments in the recent economic stimulus bill, it is not impossible.[98] Progress is indeed possible, although we are starting from a relatively low baseline.

In June 2007, the U.S. Government Accountability Office (GAO) identified significant weaknesses in all information security controls protecting federal information systems,[99] and charged that most agencies had not implemented controls to sufficiently prevent, limit, or detect access to computer networks.[100] The GAO broke the weaknesses into five major categories: (1) access controls, which ensure that only authorized individuals can read, alter and delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer dependent operations; and (5) agency wide information security programs, which provide the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.[101] According to the GAO, data losses are preventable through the implementation of adequate access controls, such as passwords, access, privileges, encryption and audit logs.[102] But because most agencies did not routinely implement these techniques, federal information system controls suffered from persistent weaknesses.[103]

Even before the GAO issued its 2007 indictment, however, the federal government had begun to make significant progress, at least on paper, in the prevention of data breaches, although not so much on compensation and cure.[104] The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide security for the information systems that support the operations and assets of the agency, including those provided or managed by

98. *See supra* text accompanying notes 71-73.
99. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 40, at 10.
100. *Id.* at 2.
101. *Id.* at 10.
102. *Id.* at 11.
103. *Id.* at 11-12, 14.
104. *See infra* text following note 117.

another agency, contractor, or other source.[105] The federal government has begun to take this duty more seriously over the past three years, in large part due to prodding from the Office of Management and Budget (OMB). OMB is responsible for establishing government-wide policies and for providing guidance to agencies on how to implement the provisions of FISMA, the Privacy Act, and other federal information security and privacy laws.[106] Under FISMA, and even more so under the OMB's guidance, agencies are required to do cost-benefit analyses, and to provide security "commensurate with the risk and magnitude of the harm" resulting from possible data breaches and other security risks.[107]

Much remains to be done. According to the 2008 ITRC report, "only 2.4% of all breaches had encryption or other strong protection methods in use. Only 8.5% of reported breaches had password protection. It is obvious that the bulk of breached data was unprotected by either encryption or even passwords."[108] This was so despite a 2006 OMB directive requiring agencies to encrypt and otherwise protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter:

> 1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
>
> 2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
>
> 3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
>
> 4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive da-

105. Federal Information Security Management Act, 44 U.S.C. § 3544(b) (2006).

106. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION, GAO 08-343, at 13 (Jan. 2008), *available at* http://www.gao.gov/new.items/d08343.pdf.

107. 44 U.S.C. § 3544(a)(1)-(2) (2006).

108. Identity Theft Resource Center, 2008 *Breach Total Soars* (Jan. 6, 2009), http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml. The ITRC aggregated breaches from the public and private sectors, so it is conceivable that the government-only statistics would be somewhat better, but because the public sector (government and much of what ITRC calls "education") represented about half of the sample set the numbers in the text are likely to be representative of the government's performance.

ta has been erased within 90 days or its use is still required.[109]

These appear to be sensible requirements, but it has taken time to get the federal bureaucracy to adhere to them.[110]

As of 2007, every federal agency has been required to create a "breach notification policy."[111] For example, the U.S. Equal Employment Opportunity Commission's (EEOC) policy includes a number of useful prophylactic measures, such as the removal of SSNs from the electronic records of people who file employment discrimination charges.[112] It also requires an annual internal review of "the current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely and complete and reduce them to the minimum necessary for the proper performance of the agency function."[113] And the agency pledges to include these reviews in its annual FISMA report.[114]

Regarding breaches, the EEOC policy reiterates the OMB rule that any breach must be reported to the U.S. Computer Emergency Readiness Team (US-CERT) within an hour of discovery. Public notification moves less quickly. The OMB requires only that the victims be notified "without unreasonable delay" and "consistent with the needs of law enforcement and national security and any measures necessary for your agency to determine the scope of the breach."[115] The OMB rule gives agency heads, or their designates in writing, the authority to delay notification but cautions that "delay should not exacerbate risk or harm to any affected individual(s)."[116]

Even worse, and echoing the OMB's general silence on the subject, the EEOC's compensation menu is rather meager: the agency will decide if credit monitoring will be offered for affected individuals.[117] There are no provisions

---

109. Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., OFFICE OF MGMT. & BUDGET, ON PROTECTION OF SENSITIVE AGENCY INFORMATION, M-06-16, at 1 (Jun. 23, 2006), *available at* http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

110. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 106, at 1-4.

111. Memorandum from Clay Johnson III, Deputy Dir. For Mgmt., OFFICE OF MGMT. & BUDGET, ON SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION, M-07-16, at 1 (May 22, 2007), *available at* http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf (requiring all agencies to "to develop and implement a breach notification policy **within 120 days**") (bold and underlining in original) [hereinafter Johnson Memorandum].

112. The U.S. Equal Employment Opportunity Commission, Breach Notification Policy, http://www.eeoc.gov/breach/breach_notification_policy.html (last modified Sept. 25, 2007) [hereinafter EEOC Notification Policy].

113. *Id.* § 2.

114. *Id.*

115. Johnson Memorandum, *supra* note 111, at 16.

116. *Id.*

117. EEOC Notification Policy, *supra* note 112, at § III(B) ("If the breach includes social

for additional compensation. The closest thing to a compensation requirement in the federal administrative breach regime is the suggestion, which lacks force of law, in the President's Identity Theft Task Force's Strategic Plan, issued April 2007, that criminal laws be amended to ensure restitution for the value of time spent coping with identity theft.[118]

In a January 2008 report, the GAO testified that while there were improvements in information security, not all agencies had followed the OMB guidance.[119] The GAO also found that this gap in the various agencies' policies and procedures reduced the ability to protect personally identifiable information from improper disclosure.[120] There is still substantial variation in agency policies and procedures on information security. Until best practices become more standardized, data breaches from federal government databases, not to mention the states, will continue. As a result, the question of appropriate remedies will not go away.

III. NEW LEGAL REMEDIES AND OLD STUMBLING BLOCKS

Publicity helps mitigate the harms caused by breaches of personal data by putting victims and potential victims on notice that they are at risk. But notice alone is far from full mitigation, much less compensation, for the harms caused by a data breach. Currently, only the Privacy Act offers victims of a federal data breach any reasonable hope of compensation. State laws vary, but to the extent that states have allowed themselves to be sued, the would-be plaintiff will often need to characterize the harm as a tort, or a violation of state law.

This Part begins with a review of the constitutional basis for a right of information privacy. I argue below that there is a constitutional right, either free-standing or based in Due Process, limiting the government's ability to disclose personal data lawfully acquired under legal compulsion, at least in cases where the government failed to take reasonable precautions. This right is separate from any informational privacy rights that constrain the government's ability to acquire personal or corporate information.

---

security numbers or other highly sensitive information, the Core Management Group will determine whether credit-monitoring services will be offered to the affected parties at government expense.").

118. PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN 50 (2007), *available at* http://www.idtheft.gov/reports/StrategicPlan.pdf.

119. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 106, at 4.

120. *Id.* at 19 ("Agencies' implementation of OMB's guidance on personally identifiable information . . . will be essential in improving the protection of personally identifiable information.").

The key holding is *DeShaney*, which sets out a distinction between cases where the government is not liable because private parties retain freedom of action, and those where the government is liable because the government has, in effect, occupied the field.[121] In the case of government data breaches, the government has taken full control of the data; under the *DeShaney* distinction, the government is responsible when it mis-handles the data. If this is correct, then victims of many privacy breaches have a claim under section 1983 against states. Unfortunately, similar constitutional claims against the federal government would require a *Bivens* action, and the Supreme Court has narrowed *Bivens* to a point that makes the federal version unlikely to succeed.[122] As a result, persons injured by federal data breaches will have substantially inferior remedies available to them. Even where claims are possible, however, plaintiffs will need to surmount a valuation problem caused by a judicial suspicion of probabilistic harms—possible harms that may not occur but nonetheless warrant preventive action.

A. CONSTITUTIONAL THEORIES

1. Constitutional Privacy Rights Against Government Disclosure of Private Facts

The Supreme Court's major modern discussion of an informational privacy right remains *Whalen v. Roe*.[123] In *Whalen*, the Court accepted that the right to privacy includes a general "right to be let alone,"[124] which includes "the individual interest in avoiding disclosure of personal matters."[125] Despite finding a theoretical right to avoid disclosure of intimate personal matters in *Whalen*, the Court upheld a New York State statute which required that doctors provide the state with a copy of every prescription for certain drugs, and disclose the names of the patients to whom they were prescribed.[126] These data would be entered into a computerized list.[127] The decision claimed to balance the social interest in informational privacy against the state's "vital

121. 489 U.S. 189, 200 (1989).

122. *See infra* Section III.B.2.

123. 429 U.S. 589 (1977). For an interesting critique suggesting that *Whalen's* intellectual influence has largely been maligned, see Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J.L. & TECH. 194, 210-14 (2007-2008).

124. 429 U.S. at 599 (citing Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

125. 429 U.S. at 598-99 (acknowledging the existence of the right, but finding that it could be overcome by a narrowly-tailored program designed to serve the state's "vital interest in controlling the distribution of dangerous [prescription] drugs").

126. *Id.* at 603-04.

127. *Id.* at 593, 603-04.

interest in controlling the distribution of dangerous drugs."[128] Finding New York's program to be narrowly tailored, and replete with security provisions designed to reduce the danger of unauthorized disclosure, the Supreme Court held that the statute was constitutional.[129] The Court allowed the mandatory compilation and disclosure of prescription data, but it left the door open to future restrictions in light of technical change, noting that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal data in computerized data banks or other massive government files."[130] In so doing, the Court set the stage for claims that the Constitution embodies a right to informational privacy.[131]

Indeed, lower courts have interpreted *Whalen* this way.[132] Several courts have found a violation of a constitutional privacy right in the public disclosure of private medical information.[133] Ohio recognized a constitutional right

---

128. *Id.* at 598.

129. *Id.* at 601-04.

130. *Id.* at 605.

131. *See, e.g.*, Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 155, 158 (1991) (concluding that because most theories of personhood assume personal information is a crucial part of a person's identity, there should be a recognized right to informational privacy based on personhood and that since information is property, it should be protected by the Fifth Amendment); Gary R. Clouse, Note, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 541-47 (1982) (tracing the development of the right to informational privacy, and noting the Supreme Court's use of a balancing test in *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425 (1977), to determine whether an individual's constitutional rights have been infringed by a government-mandated disclosure of information); Gilbert, *supra* note 95, at 1381-88 (surveying cases in the courts of appeal that apply *Whalen's* informational privacy right).

132. For example, cases following on from *Whalen* include: *Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 551 (9th Cir. 2004) (holding that a statutory provision enabling the state to access abortion clinic patients' medical records violated patients' right to informational privacy); *Cooksey v. Boyer*, 289 F.3d 513, 515-16 (8th Cir. 2002) (overturning district court grant of summary judgment and noting that disclosure of personal information might violate the right to privacy); *Powell v. Schriver*, 175 F.3d 107, 111-112 (2d Cir. 1999) (holding that a transsexual inmate had a privacy right of confidentiality in medical records); *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."); *Eastwood v. Department of Corrections of Oklahoma*, 846 F.2d 627, 630-31 (10th Cir. 1988) ("[A variety of provisions in the Bill of Rights] protects two kinds of privacy interests: the individual's interest in avoiding disclosure of personal matters and the interest in being independent when making certain kinds of personal decisions."); *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."); *Taylor v. Best*, 746 F.2d 220, 225 (4th Cir. 1984) (recognizing that the right to privacy includes avoiding disclosure of personal facts); *Slayton v. Willingham*, 726 F.2d 631, 635 (10th Cir. 1984) (holding that the Supreme Court explicitly recognized the constitutional right to privacy in *Whalen v. Roe*).

133. *See, e.g.*, *In re* Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) (HIV status

of privacy in Social Security Numbers.[134] And the Fifth Circuit found a right against disclosure of "the most private details of [a plaintiff's] life" that had been revealed to state investigators who represented that testimony was absolutely privileged under Florida law and that the contents of his testimony would be revealed to no one.[135] On the other hand, the Sixth Circuit refused to include informational privacy among constitutionally protected interests.[136]

Whalen is more significant for what it foreshadowed than for what it held. Yes, the plaintiff lost: his privacy interest was not strong enough to outweigh the state's interest in drug laws. But because *Whalen*'s plaintiff lost on a balancing test rather than for failing to state a claim, the *Whalen* decision established the principle that there could be an actionable constitutional right to information privacy. Presumably, with the right facts, and perhaps relying on the technical change the Court foresaw in *Whalen*, a claim that the Fourteenth Amendment's protection of privacy included a right to the "nondisclosure of private information"[137] might succeed.

The right to information privacy first enunciated in *Whalen* can be characterized as a component of substantive Due Process,[138] but it is perhaps best understood as a free-standing constitutional right. The *Whalen* court itself was somewhat unclear on the issue, but a series of footnotes suggest that it draws on several parts of the Constitution.[139] Starting with *Griswold v. Connecticut*,[140] and running through *Roe v. Wade*[141] and *Planned Parenthood v. Casey,*[142] the Supreme Court has characterized the broader constitutional right to decisional privacy as having multiple sources, one of which is substantive Due Process. The two privacy rights—informational (*Whalen*) and decisional (*Roe* and *Ca-*

---

disclosure); Doe v. Attorney General of the U.S., 941 F.2d 780, 795-96 (9th Cir. 1991) (collecting cases); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990) (recognizing right to informational privacy for information related to an individual's fundamental rights and "[p]ersonal, private information in which an individual has a reasonable expectation of confidentiality").

134. *See* State *ex rel.* Beacon Journal Publ'g Co. v. City of Akron, 640 N.E.2d 164, 169 (Ohio 1994) (relying in part on section 7 of the Privacy Act).

135. Fadjo v. Coon, 633 F.2d 1172, 1175-76 (5th Cir. 1981).

136. *See* Lambert v. Hartman, 517 F.3d 433, 445 (6th Cir. 2008) (driver whose identity was stolen as result of clerk of court's publication of her Social Security Number on public website did not have a constitutionally protectable fundamental property interest in her personal information that might serve as basis for substantive Due Process claim); J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981) (compilation and dissemination of social histories prepared by state probation authorities in connection with proceedings involving juveniles).

137. Whalen v. Roe, 429 U.S. 589, 600 (1977).

138. *DeSanti*, 653 F.2d at 1088-89 (tying *Whalen* to substantive Due Process).

139. *See Whalen*, 429 U.S. at 600 nn.23-25.

140. 381 U.S. 479 (1965).

141. 410 U.S. 113 (1973).

142. 505 U.S. 833 (1992).

sey)—are not the same, but they are often conflated;[143] to the extent they are further conflated, the informational privacy right may come to be understood as part of Due Process rather than a free-standing right. Indeed, a number of circuits seem to see it that way.[144]

Supreme Court decisions following *Whalen* appear to agree that there is or ought to be a zone of constitutionally protected informational privacy, even if the Court has yet to encounter data that is entitled to remain in that zone. In *Nixon v. Administrator of General Services*, the Court applied *Whalen*'s balancing test to reject President Nixon's claim that allowing government archivists to review and classify his presidential papers and effects violated his "fundamental rights . . . of . . . privacy."[145] Nixon's privacy interest was found insufficiently strong to outweigh the public interest in preserving his papers.[146] Similarly in both *Cox Broadcasting Corp. v. Cohn*[147] and *Florida Star v. B.J.F.*,[148] the Court struck down state law privacy claims arising from the accurate publication of arguably private facts that had become matters of public record. But in so doing, the Court did suggest that "there is a zone of privacy surrounding every individual,"[149] even if did not say where that zone was or what might occupy it.

---

143. *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 530 (2006) (stating that "[*Whalen*] recognized that the 'right of privacy' [was] based on substantive due process").

144. *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) (Table case 39 F.3d 320) (holding 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) (Table case 946 F.2d 895) ("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.").

145. 433 U.S. 425, 455-57 (1977).

146. *Id.* at 465.

147. 420 U.S. 469, 495-97 (1975).

148. 491 U.S. 524, 540-41 (1989) (concerning name of rape victim erroneously posted by the police, then published by a newspaper in violation of a Florida statute that made it unlawful to report the name of a victim of a sexual offense).

149. *Cohn*, 420 U.S. at 487.

Also relevant is the unanimous decision in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, in which the Supreme Court held that there was a heightened privacy interest sufficient to overcome an FOIA application in an FBI compilation of otherwise public information.[150] Even if the data contained in a "rap sheet" were located in scattered courthouses as public records, the compilation itself, the "computerized summary located in a single clearinghouse," was not available to the public.[151]

> Because events summarized in a rap-sheet have been previously disclosed to the public, respondents contend that Medico's privacy interest in avoiding disclosure of a federal compilation of these events approaches zero. We reject respondents' cramped notion of personal privacy. To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus, the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private.[152]

Reporters Committee is obviously not a constitutional decision as it merely interpreted a FOIA exception, but it does suggest that, even in 1989, the Court understood that databases can have privacy consequences.

Subsequent Supreme Court cases touching on informational privacy have not changed the basic contours set up by these fundamental cases, although they have filled in some of the details.[153] In the course of upholding a federal

---

150. 489 U.S. 749, 780 (1989).

151. *Id.* at 764.

152. *Id.* at 764-65.

153. In *Bartnicki v. Vopper*, the Court held that privacy claims must give way to the First Amendment "interest in publishing matters of public importance." 532 U.S. 514, 534 (2001). Both *Whalen* and *Bartnicki* are opinions by Justice Stevens, and there is nothing in the 2001 opinion to suggest any retreat from *Whalen*'s 1977 formulation, although *Whalen* is not cited. Justice Stevens did note,

> It seems to us that there are important interests to be considered on *both* sides of the constitutional calculus. In considering that balance, we acknowledge that some intrusions on privacy are more offensive than others, and that the disclosure of the contents of a private conversation can be an even greater intrusion on privacy than the interception itself. As a result, there is a valid independent justification for prohibiting such disclosures by persons who lawfully obtained access to the contents of an illegally intercepted message, even if that prohibition does not play a significant role in preventing such interceptions from occurring in the first place.

statute protecting private information, *Reno v. Condon* treated the regulation of state driver's license databases much like the regulation of ordinary property.[154] *Whalen*'s holding that data privacy is a value of constitutional import endures, albeit in a somewhat latent form as the right is still waiting for its first triumph over countervailing factors in the Supreme Court. As noted above, however, several Circuit Courts have clearly stated that *Whalen* creates a constitutional right to privacy, one that can determine outcomes.[155]

2. The Substantive Due Process Aspect of the Right

A person or firm whose data has been exposed by the government has suffered a compensable deprivation of life, liberty, or property without Due Process of law if the government took on an obligation to keep the data confidential.[156] How to characterize that doctrinally, and in precisely which circumstances current doctrine may permit a remedy, are surprisingly complex questions for what should, morally, be a fairly simple matter. The government may have taken the information by force of law, or because it is the only game in town. The government's promise to safeguard the information may be statutory, regulatory, or in some cases implicit.[157] But if the failure to safeguard the data was negligent or lacked of elementary due care, as opposed to the result of the intervention of a criminal so accomplished that his actions could not reasonably be foreseen, then the government should make restitution.

Begin with a relatively simple case: Suppose that the data in question

---

Id. at 533.

154. Reno v. Condon, 528 U.S. 141, 148 (2000) ("Because drivers' information is, in this context, an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation.").

155. *See supra* text accompanying notes 132-135.

156. One example is the disclosure of a SSN. The Social Security Act, which requires the use of SSNs for disbursement of benefits, declares that SSNs obtained or maintained by authorized individuals on or after October 1, 1990, are confidential and prohibits their disclosure. 42 U.S.C. § 405(c)(2)(C)(viii)(I) (2006). It is common to speak of a person "owning" their SSN. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD, GAO/T-HEHS-00-111, at 3 (May 9, 2000), *available at* http://www.gao.gov/new.items/he00111t.pdf.

157. A survey of how the government makes binding confidentially promises is beyond the scope of this essay. As a general matter, an oral or even written representation by a government official in many cases will not suffice since it is hornbook law that an official without authority to make a binding representation cannot estop the government. *See* Office of Pers. Mgmt. v. Richmond, 496 U.S. 414, 419-20 (1990). I would argue, however, that a representation by an authorized person would suffice, as would promises made in certain special circumstances such as plea bargaining. *See* Fadjo v. Coon, 633 F.2d 1172, 1175-76 (5th Cir. 1981) (finding right against disclosure of facts being revealed to state investigators after representation that testimony would be revealed to no one).

clearly belonged to the data subject. The subject disclosed it to the government either because it was required or because it was a necessary condition precedent to a government license or benefit.[158] Assume further that a government employee loses a copy of the data by failing to exercise basic care: perhaps a computer was left unsecured, data was accidentally posted to a public web site, or an employee lost control of an unencrypted USB drive. Note that these hypotheticals have a common feature: they don't involve a hacker, much less a movie-quality hacker, or über-criminal.[159] Indeed, they involve great negligence, and perhaps in some cases, gross negligence. As described below, Due Process may not protect the public against theft of data entrusted to the government when the theft is carried out by unusually skilled hackers. The Due Process Clause requires that the government exercise only due care, not perfect care. And even when the government has been only negligent, recovery may be difficult.

The disclosure of private information has a negative impact on the owner or subject of the data. In some cases the data breach threatens to reduce, perhaps to zero, the value of the formerly secret data, destroying much or all of the value of an information asset such as a trade secret. Alternately, the damage could be purely due to secondary effects, such as actual or potential identity theft. In these cases, the data itself is not necessarily reduced in value, but rather the person who acquires it gains the power to cause harm.[160] In either case, there is actual or probabilistic harm.

A harm is probabilistic if it is unknown whether it will occur, or how severe it will be. At the time the government discovers it has lost control over the data, neither it nor the subject may know whether the data has in fact been acquired by anyone else. That a laptop has been lost does not mean it will be found by a malicious third party. That a USB drive is returned by a seemingly good Samaritan does not exclude the possibility that the contents were copied before their return. That data was put on a public website viewed by several dozen people does not tell us whether the people had any

158. The data might, for example, be information attached to a tax return, an EEOC complaint, or personal data disclosed by a probationer or by a government employee, or a trade secret disclosed pursuant to the Federal Insecticide, Fungicide, and Rodenticide Act. The Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) requires manufacturers seeking government registration of pesticides to disclose health, safety, and environmental data to the Environmental Protection Agency. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1007 (1984) (characterizing disclosures as voluntary).

159. On the dangers of focusing on this unrealistic case, see generally Paul Ohm, *The Myth of the Super-User: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327 (2008).

160. This can be a complex issue. Sometimes the data will have no intrinsic value (e.g. a password) or sometimes its value will be unchanged (e.g. the number of a bank account), but the disclosure will nonetheless be harmful.

interest in it or if they copied the data. Yet, even in cases where the release only creates a *risk* of harm, the subject must expend resources on monitoring and prevention so long as the expected value of the risk is sufficiently great to justify the expense.[161]

The key case in establishing the contours of the Due Process right to compensation for certain government data breaches is Chief Justice Rehnquist's opinion in *DeShaney*.[162] Chief Justice Rehnquist is an unexpected source for a major information privacy right, and *DeShaney* is a particularly unexpected locus for its elucidation. *DeShaney* is notorious as an opinion in which the Supreme Court held that the state of Wisconsin had no duty under the Constitution to protect a boy, the infamous "poor Joshua" of Justice Blackmun's dissent,[163] from a permanently disabling beating by his father.[164] The absence of a duty was controversial because the state social services were on actual notice that Joshua had been repeatedly injured and was at risk.[165] In finding that the Due Process clause imposed no duty of care on state social services regarding children residing with a parent, at least absent a statutory or regulatory undertaking to protect children from their parents, Chief Justice Rehnquist distinguished Joshua's case from one where a duty would have existed. Mere notice was not enough; the state would have had a duty only if it had placed Joshua in circumstances where it "renders him unable to care for himself, and at the same time fails to provide for his basic human needs . . . ."[166] The duty arises "from the limitation which it has imposed on his freedom to act on his own behalf" not "its failure to act to protect his liberty interests against harms inflicted by other means."[167] Chief Justice Rehnquist

161. On the valuation issue, see *infra* Section III.C.

162. 489 U.S. 189 (1989). I am grateful to Patrick Gudridge for pointing out the centrality of *DeShaney* in this context.

163. *Id.* at 213 (Blackmun, J., dissenting).

164. *Id.* at 191.

165. *See id.* at 192-93.

166. *Id.* at 200.

167. *Id.* The full quotation is:

> [W]hen the State by the affirmative exercise of its power so restrains an individual's liberty that it renders him unable to care for himself, and at the same time fails to provide for his basic human needs—*e.g.,* food, clothing, shelter, medical care, and reasonable safety—it transgresses the substantive limits on state action set by the Eighth Amendment and the Due Process Clause. The affirmative duty to protect arises not from the State's knowledge of the individual's predicament or from its expressions of intent to help him, but from the limitation which it has imposed on his freedom to act on his own behalf. In the substantive due process analysis, it is the State's affirmative act of restraining the individual's freedom to act on his own behalf-through incarceration, institutionalization, or other similar restraint of personal liberty-which is the "deprivation of liberty"

immediately added in a footnote that, "[e]ven in this situation, we have recognized that the State 'has considerable discretion in determining the nature and scope of its responsibilities.'"[168]

When the State takes a person's data and holds it in a fashion outside the person's control, the State has done to that data exactly what Chief Justice Rehnquist said was necessary to trigger Due Process Clause protection: it has "by the affirmative exercise of its power" taken the data and "so restrain[ed]" it that the original owner is unable to exert any control whatsoever over how the government stores or secures it.[169] The government's "affirmative duty to protect" the data "arises . . . from the limitation which it has imposed on his freedom to act on his own behalf" to keep the data secure.[170] Again, "it is the State's affirmative act of restraining the individual's freedom to act on his own behalf" which creates a duty on the government to keep the data secure.[171] The State created the danger, and thus the State is responsible for the outcome.[172]

One might object that the *DeShaney* holding stands for the proposition that when the government stands by and lets another do harm to a person, that person has no recourse unless the government has taken on an affirmative duty to protect. In this view, exposing private data on the web or losing an unencrypted database is not the harm. Rather, the harm comes from a third party's use of the data, something for which this reading of *DeShaney* says the government should not be blamed. But this is a misreading of *DeShaney* because the analogy is incorrect. In *DeShaney*, the State had no duty because it had never taken Joshua into care.[173] The harms he suffered at his father's hands were private wrongs, a direct transaction in which the government had no part.[174] The Chief Justice characterized the State as an absent party:

> The most that can be said of the state functionaries in this case is that they stood by and did nothing when suspicious circumstances dictated a more active role for them. In defense of them it must al-

---

> triggering the protections of the Due Process Clause, not its failure to act to protect his liberty interests against harms inflicted by other means.

Id. (citations omitted).

168. *Id.* at 200 n.7.

169. *See id.* at 200.

170. *See id.*

171. *See id.*

172. *Cf.* Michele H. Berger, Comment, *Negligence Or State-Created Danger: Two Avenues For Injured Student Informants Pursuing School Liability*, 30 U. LA VERNE L. REV. 94, 96-104 (2008) (discussing effects of "state-created danger doctrine" in the context of schools).

173. *See DeShaney*, 489 U.S. at 199-200.

174. *See id.* at 201.

> so be said that had they moved too soon to take custody of the son away from the father, they would likely have been met with charges of improperly intruding into the parent-child relationship, charges based on the same Due Process Clause that forms the basis for the present charge of failure to provide adequate protection.[175]

Indeed, it was the claim that the government had a duty to intervene which was the heart of the plaintiff's case, and which the majority rejected.[176]

Contrast this to a hypothetical lost database: there is no question that the government had taken full control of the data before it lost them. Once the government takes that control, the subject of the data is completely disempowered with regards to how the data will be protected. Therefore, it is nonsensical to suggest that when the government negligently allows a third party to access the data, that third party is the only relevant actor for Due Process purposes. The government remains the critical intermediary, the one actually responsible for allowing the loss. In the case of information controlled by the government, it is not a bystander, but rather a direct agent. The government's active role in controlling the data, one that displaces the subject or owner of the data, is what creates the duty of care. Or as the Seventh Circuit stated, "The state must protect those it throws into snake pits, but the state need not guarantee that the volunteer snake charmer will not be bitten."[177]

The relevant law here is substantive, not procedural, Due Process. Interestingly, however, the answer would be about the same under a procedural Due Process standard. Procedural Due Process is not a fixed quantum but a sliding scale, one that alters with the circumstances. The leading case on how much process is due remains *Mathews v. Eldridge*.[178] Although it was originally a property-rights test, a plurality of the Supreme Court recently applied the *Mathews* test to a liberty interest in *Hamdi v. Rumsfeld*.[179] The plurality used *Mathews* to set up a three-part balancing test: weighing "the private interest that will be affected by the official action" against the Government's asserted interest, "including the function involved" and the burdens the Government would face in providing greater process.[180] The *Mathews* calculus then contemplates balancing of these concerns, through an analysis of "the risk of an erroneous deprivation" of the private interest if the process were reduced and the "probable value, if any, of additional or substitute safeguards."[181]

---

175. *Id.* at 203.
176. *See id.*
177. Walker v. Rowe, 791 F.2d 507, 511 (7th Cir. 1986).
178. 424 U.S. 319 (1976).
179. 542 U.S. 507, 529-31 (2004) (plurality opinion).
180. *Id.* at 529 (quoting *Mathews*, 424 U.S. at 335).
181. *Id.*

The *Mathews* test has justly been criticized for requiring courts to balance incommensurable qualities.[182] And it is indeed no bright line. But in the context of data security, it must surely encompass at least an industry-standard level of care. Failing to update software, placing private data in public files online, losing laptops, tapes, or USB drives with unencrypted (or weakly encrypted) data are all so far below the basic standard of care as to be actionable. Indeed, one could reasonably argue that the federal government's evolving, and improving, guidelines for the storage of personal data creates a standard to which state government should also be held.

On the other hand, the *Mathews* test would produce a much less victim-friendly picture when data breaches are caused by a malicious and skilled hacker as opposed to an opportunistic third party taking advantage of government carelessness. If, despite reasonable security precautions, a government database is hacked, especially from the outside the government would be able to argue that the real cause of the breach is external, exceptional, and unpredictable.[183] In many of these "smart hacker" cases, the government would likely be able to convince a court that additional security sufficient to prevent this previously unknown threat would not have been a reasonable expenditure. And that, as we will see, is also, more or less, the substantive Due Process result.

B. MODES OF RECOVERY

If the informational privacy right first alluded to in *Whalen* is indeed actionable in cases where the government failed to exercise due care, then there could be no better place to put it into action than to use it to remedy damages caused by accidental or illegal government data breaches. In *Whalen* the data were kept for lawful purposes. In the data breach scenario, the harm is not keeping the data, which presumably is also held for a lawful purpose, but rather it is an accidental or illegal disclosure. Establishing that the right exists is not enough, however, as the modern Supreme Court has erected doctrines that complicate any attempt at recovery, both under section 1983 against a state, and under *Bivens* against the federal government.

1. Section 1983 Action Against a State

If, as I have argued above, the right to have one's data looked after properly is indeed based in the Constitution, pleading a section 1983 claim for damages due to an actual or feared data breach should in principle be

182. *See, e.g.*, Edward L. Rubin, *Due Process and the Administrative State,* 72 CALIF. L. REV. 1044, 1136-44 (1984).

183. Inside jobs raise questions of due care in supervision and in the deployment of internal controls.

straightforward.[184] But two doctrines create possible obstacles: the Supreme Court's reluctance to allow section 1983 cases involving mere negligence in substantive Due Process claims, and a valuation problem. This section considers the first issue, the availability of relief under section 1983; valuation is discussed below in Section III.C.

A negligent act by a state official leading to a data breach should be actionable under section 1983.[185] That said, the government's duty of care is not unbounded. Yet, since *DeShaney*, the Supreme Court has not decided how much the duty extends to non-custody circumstances in which the state fails to provide or maintain services. Nevertheless, most courts of appeals accept that a duty enforceable under section 1983 applies if the State creates, and even more so if it enhances, a danger, although some courts require a high standard of egregiousness.[186] On the other hand, several courts have held that even where there is a duty, the responsible party may be protected by qualified immunity if the underlying federal right was unclear.[187]

Assuming no qualified immunity, the first critical issue therefore is deciding which data breaches are properly chargeable to the government under *DeShaney*, and which result primarily from the independent actions of a third party not under government control. A second issue, still the subject of debate in the larger context of section 1983, is the extent to which a plaintiff would have to prove more than ordinary negligence, unless the fact of the government-enhanced risk suffices to establish liability.

Failing 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. In each of these cases, the but-for cause of the breach is the government's failure to meet minimal professional standards for handling sensitive data.[188] Under the *DeShaney* stan-

184. *See supra* note 45 (quoting 42 U.S.C. § 1983 (2006)). There are two elements of any section 1983 claim: the plaintiff must allege (1) a deprivation of a federal right and (2) that the person who deprived him of that right acted under color of state law. Gomez v. Toledo, 446 U.S. 635, 640 (1980).

185. Note, however, that several circuit court cases hold that the Ninth Amendment alone does not support a section 1983 claim. *See* MARTIN A. SCHWARTZ, 1 SECTION 1983 LITIGATION: CLAIMS AND DEFENSES § 3.03[B] at 3-25 n.80 (4th ed. 2003 & Supp. II 2008) (collecting cases). The Ninth Amendment is a part of the constitutional basis for a right to privacy. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

186. *See* SCHWARTZ, *supra* note 185, § 3.09[E] at 3-252.

187. *Id.* § 3.09[D] at 3-252.

188. Indeed, one could reasonably argue that the federal government's evolving and improving guidelines for the storage of personal data creates a standard to which state government should also be held. *See supra* Section II.C.

dard, these sorts of breaches should be blamed on the responsible party—the government—not the opportunistic third party who takes advantage of the responsible party's carelessness. What is more, many of these breaches will be the result of a policy, or pattern and practice, of failing to secure and patch systems, or failing to encrypt databases.

But where there is a sound policy in place requiring security, and it is routinely followed but was uncharacteristically ignored, a section 1983 claim may yet founder on the rule that mere negligence cases do not qualify for recovery. That is, unless the state-created danger rule is understood to mean that where the government steps in and forecloses self-help, mere negligence might be enough.[189] On the other hand, if the data has been kept in a reasonably secure fashion, and a skilled hacker nonetheless gets access, the breach is something external, exceptional, and unpredictable.[190] If additional security sufficient to prevent this previously unknown threat would not have been a reasonable expenditure ex ante, it is hard to see how the government can fairly be blamed.

Furthermore, a section 1983 claim requires that the person committing the deprivation have "acted under color of state law."[191] The Supreme Court has held in several contexts, however, that mere negligence by a state or local official does not give rise to a substantive Due Process claim against a state or municipality. Rather, to recover against a state government entity under section 1983 there must be an intentional or deliberate deprivation of life, liberty, or property,[192] or at least "deliberate indifference."[193]

The deliberate indifference requirement need not be fatal. As noted

---

189. *See e.g.*, Butera v. District of Columbia, 235 F.3d 637, 653 (D.C. Cir. 2001) (collecting cases).

190. Inside jobs raise questions of due care in supervision and in the deployment of internal controls.

191. 42 U.S.C. § 1983 (2006).

192. *See* Daniels v. Williams, 474 U.S. 327, 328-330 (1986); *see also* Davidson v. Cannon, 474 U.S. 344, 347-48 (1986) (explaining *Daniels*). The Court subsequently limited the reach of this doctrine when state actors infringe rights other than the Due Process Clause. *See e.g.*, Graham v. Connor, 490 U.S. 386, 395, 397 (1989) ("Today we make explicit . . . that *all* claims that law enforcement officers have used excessive force . . . in the course of an arrest, investigatory stop, or other 'seizure' of a free citizen should be analyzed under the Fourth Amendment and its 'reasonableness' standard, rather than under a 'substantive Due Process' approach," and "the 'reasonableness' inquiry in an excessive force case is an objective one . . . without regard to their underlying intent or motivation.").

193. City of Canton v. Harris, 489 U.S. 378, 388 (1989) (pre-*Collins v. City of Harker Heights*, 503 U.S. 115 (1992), decision finding municipal liability for poor training where failure to train amounted to deliberate indifference to the rights of persons whom the police come into contact); Estelle v. Gamble, 429 U.S. 97, 106 (1976) (deliberate indifference "to a serious medical need").

above, in the case of a data breach, the State's total control of the data, and its enhancement of the risk that the data may be disclosed, imposes an additional burden that it would not have in ordinary circumstances.[194] Alternately, the State's action in taking and holding the data can fairly be characterized as having subjected it to a heightened risk of improper disclosure, invoking the 'enhancement of risk doctrine' adopted by some courts of appeals.[195] In addition, a significant fraction of state breach cases to date are more systematic than the low-level, one-off negligence situations that the Supreme Court seemed concerned about in *Daniels v. Williams*.[196] A failure to have an adequate policy reasonably calculated to prevent data breaches, or a failure to require encryption of stored (and especially transported) data could transform a lost laptop or an improperly accessed server case into a section 1983 pattern-and-practice or deliberate indifference issue.

As this article went to press, the Supreme Court added a potentially more severe difficulty by holding in *Ashcroft v. Iqbal* that all section 1983 (and *Bivens*) plaintiffs must plead that each Government defendant, through his own individual actions, violated the Constitution.[197] The Court rejected the argument that a government official could be liable under a theory of "supervisory liability."[198] How this will play out in the context of government data breaches remains to be seen. Claims traceable to an individual's action—say, a lost laptop—certainly will be simpler to plead than those involving a more systemic failure, such as a department's failure to maintain its software or to properly train staff in its use. As noted above, however, even that simpler case may require a showing of deliberate indifference or its equivalent.

2. Bivens

In *Bivens v. Six Unknown Federal Narcotics Agents*, the Supreme Court found (or created) a federal cause of action for damages resulting from federal agents' violations of the Fourth Amendment.[199] In the almost fifty years since *Bivens*, the Supreme Court has extended it only twice: once to find an implied damages remedy under the Due Process Clause of the Fifth Amendment in

194. *See* SCHWARTZ, *supra* note 185, § 3.09[E] at 3-255 (surveying appellate cases and establishing that "[m]ost of the circuit courts have adopted some version of the state-created danger doctrine").

195. *See supra* notes 186, 194.

196. *See* 35 DAVID B. BROOKS, TEXAS PRACTICE SERIES, COUNTY AND SPECIAL DISTRICT LAW § 2.31 (2d ed. 2008) ("The issue which is the essence of most § 1983 litigation against local government today is whether the conduct of public officials or employees constitutes governmental policy or custom.").

197. 129 S. Ct. 1937, 1948 (2009).

198. *Id.* at 1949.

199. 403 U.S. 388, 391, 396-97 (1971).

Davis v. Passman,[200] and once to find a remedy under the Cruel and Unusual Punishment Clause of the Eighth Amendment in *Carlson v. Green*.[201] Both cases, however, were decided decades ago, and the more modern Court has evinced more than a slight hostility to new *Bivens* arguments.[202] Thus, for example, the Court has firmly resisted efforts to extend *Bivens* to suits requesting remedies from an entire federal agency, stating that *Bivens*' only purpose is to deter individual federal officers.[203] Justice Scalia, in particular, has made no secret of his disdain for *Bivens*, writing (with Justice Thomas):

> I do not mean to imply that, *if* the narrowest rationale of *Bivens did* apply to a new context, I *would* extend its holding. I would not. *Bivens* is a relic of the heady days in which this Court assumed common-law powers to create causes of action—decreeing them to be "implied" by the mere existence of a statutory or constitutional prohibition. As the Court points out . . . we have abandoned that power to invent "implications" in the statutory field. There is even greater reason to abandon it in the constitutional field, since an "implication" imagined in the Constitution can presumably not even be repudiated by Congress.[204]

While *Bivens* remains good law in regard to remedies for egregious rights violations by federal law enforcement officers, there is little reason to believe that the Supreme Court would allow *Bivens* to expand outside its current narrow confines, and particularly little reason to expect expansion in the information privacy context.

Even if the Court were less hostile to *Bivens* claims, it is unclear that the rationale of the *Davis* and *Carlson* cases would apply to the information privacy context. In both those cases, the Supreme Court stressed the absence of any alternate equally effective form of relief.[205] That may doom *Whalen*-based

---

200. Davis v. Passman, 442 U.S. 228, 231, 234 (1979) (recognizing Due Process clause claim alleging right to be free from gender discrimination as cause of action under the Fifth Amendment). *Contra* Schweiker v. Chilicky, 487 U.S. 412, 421-24 (1988) (declining to extend *Bivens* to alleged Fifth Amendment violations stemming from Social Security claims).

201. 446 U.S. 14, 18-20 (1980). *Carlson* represents perhaps the greatest, and also last clear expansion of *Bivens*. *But c.f.*, Bush v. Lucas, 462 U.S. 367, 377-79 (1983) (declining to extend *Bivens* to alleged First Amendment violation of federal employees' rights by their supervisor at a federal agency).

202. *See, e.g.*, Corr. Servs. Corp. v. Malesko, 534 U.S. 61, 71-72 (2001) (rejecting attempt to find implied private right of action, pursuant to *Bivens*, for damages against private operator of halfway house acting under color of federal law).

203. FDIC v. Meyer, 510 U.S. 471, 485 (1994).

204. *Malesko*, 534 U.S. at 75 (Scalia, J., concurring) (citations omitted).

205. *Carlson*, 446 U.S. at 20-21 (noting that "*Bivens* remedy is more effective than the Federal Tort Claims Act (FTCA) remedy"); Davis v. Passman, 442 U.S. 228, 231, 245 (1979).

claims because when it comes to information privacy claims against the federal government, the public enjoys the Privacy Act, despite all its flaws. Indeed, the District of Columbia Circuit recently rejected a *Bivens* data privacy claim for just this reason, noting that the Privacy Act constitutes a "comprehensive statutory scheme" that precludes such suits, and that the "plaintiffs could have stated colorable Privacy Act claims based on some of the alleged disclosures."[206] Other circuits have been more willing to hold that *Whalen* creates an enforceable privacy right,[207] but outside the context of law-enforcement, prison, or parole related cases, and perhaps medical privacy (*Whalen*'s facts), the Supreme Court will likely remain unwilling to follow suit.

C. THE VALUATION PROBLEM

Whether plaintiffs rely on *Bivens* or section 1983, valuation issues present a special problem in information breach cases for two reasons. First, the injuries likely will be as diffuse as the number of people or firms whose data was unintentionally exposed.[208] Second, in many breach cases it is not immediately clear how many people accessed the data nor whether they will make use of it. The harms from a data breach are sometimes immediate, but they are often speculative—perhaps no one saw it or an identity thief is just biding his time.

Valuation can become the critical issue when statutory remedies have threshold damages requirements. One of the possible ways to bring a claim under the Computer Fraud and Abuse Act, for example, requires $5,000 or more damage as a prerequisite to suit.[209] The statute defines damages broadly to include reasonable cost to any victim,[210] and the losses can be aggregated

206. Wilson v. Libby, 498 F. Supp. 2d 74, 87-88, 91 (D.D.C. 2007). Other courts have been more creative, at least in the law enforcement context. *See* Herring v. Keenan, 218 F.3d 1171, 1180-81 (10th Cir. 2000) (holding that *Bivens* action against probation officer for violating his probationer's informational privacy by revealing probationer's HIV-positive status to the probationer's sister and employer stated a claim but was barred by qualified immunity as right was not clearly established at time disclosure was made).

207. *See* cases cited *supra* notes 132, 131.

208. The aggregation issue is a familiar problem from the class action context, but so too is the roadblock that even when many plaintiffs suffer from a common cause, the federal courts will not as a rule entertain a case where the damages are likely to be individuated (e.g. theft from bank accounts). A federal court must find that "the questions of law or fact common to class members predominate over any questions affecting only individual members" before certifying a class. FED R. CIV. P. 23(b)(3).

209. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

210. *Id.* § 1030(e)(11). *Cf.* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) (including cost of conducting a damage assessment and hiring a security consultant among the damages); United States v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000) (including the wages of the employee who repaired the damage among the damages, even if he would have gotten the same wage regardless of whether he repaired the damage or

among victims.[211] At the time many victims learn of a data breach, however, it is uncertain as to whether they will suffer any tangible loss. The uncertainty itself is a form of damage, as a reasonably prudent person will take steps to secure their assets against third parties, such as an identity thief, who might try to use the data. Nevertheless, this idea has proved oddly difficult for some courts to accept in the data breach context, even though courts have had little trouble seeing probabilistic loss as an actionable harm in other contexts.[212] In *Pisciotta v. Old National Bancorp*, for example, the Seventh Circuit stated, "The plaintiffs maintain that the [Indiana breach] statute is evidence that the Indiana legislature believes that an individual has suffered a compensable injury at the moment his personal information is exposed because of a security breach. We cannot accept this view."[213] This is no isolated phenomenon:

> To date [2008] no court has found a plaintiff damaged by the mere release of the plaintiff's information. . . . [C]ourts have required that the information be used fraudulently. If a plaintiff can provide evidence that the plaintiff suffered an actual loss, they must still prove that this loss was caused by the breach.[214]

As noted above, federal regulations offer the possibility of credit monitoring as a practical matter, and this is what most settlements seem to offer class plaintiffs.[215] There is one notable exception to this rule, *Dickinson v. Collier*, in which class members received only one dollar each without a showing of actual damages.[216]

---

not).

211. Thus, for example, 18 U.S.C. § 1030(c)(4)(A)(I) (2006) sets the penalty for "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value."

212. *See, e.g.*, Nat'l Res. Def. Council v. EPA, 464 F.3d 1, 6 (D.C. Cir. 2006) (holding that probabilistic risk, or substantial probability, of loss conferred standing).

213. 499 F.3d 629, 637 (7th Cir. 2007).

214. Derek A. Bishop, *No Harm No Foul: Limits on Damages Awards for Individuals Subject to a Data Breach*, 4 SHIDLER J. L. COM. & TECH. 12 at ¶ 23 (2008), *available at* http://www.lctjournal.washington.edu/Vol4/a12Bishop.html.

215. *See* GOV'T ACCOUNTABILITY OFFICE, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN, GAO-07-737, at 35 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf ("Entities experiencing a breach also often provide affected individuals with free credit monitoring services."). For an overview of recent private data breach court decisions, see generally Bishop, *supra* note 214; John Kennedy & Parishi Sanjanwala, *Outside Counsel: Civil Suits Arising From Information Security Breaches*, N.Y.L.J., Feb. 2, 2007, at col. 4.

216. 477 F.3d 1306 (11th Cir. 2007).

Statutory damages should be a way of overcoming valuation difficulties. The Privacy Act offers statutory damages of $1,000 where an agency acted in a manner that was intentional or willful,[217] but as noted above, in *Doe v. Chao* the Supreme Court held that plaintiffs seeking to recover this sum from the government must prove at least some "actual damages," and that a complaint of emotional injury stemming from the disclosure of their SSNs did not suffice.[218] The government admitted that it published the plaintiff's SSNs widely.[219] At the trial court level the plaintiffs did allege that they were concerned about identity theft, but they appear to have framed this as an emotional injury claim, rather than as a probabilistic injury.[220] Thus, *Doe v. Chao*, does not directly address whether a properly pled probabilistic injury would state a claim under the Privacy Act, although the thrust of *Doe v. Chao* would seem to lean against it.

IV. CONCLUSION

Government data breaches have some similarities to private sector data losses, but there are also major differences. Governments have the power to compel data disclosures by law, and by de facto legal regimes that make disclosures a prerequisite for licenses and benefits that are required to live a normal life, or to conduct a normal business.

Data breach legislation fueled by, and fueling, an increased public concern over data breaches represents one of the important success stories over the past decade in the campaign to increase the legal protection for personal data privacy in the United States. Florida's current breach statute, for example, requires corporations to notify victims of a data breach within forty-five days, or face fines of up to $500,000 per breach.[221] While the statute does not apply to government agencies, it does cover government contractors.[222] Often, governments have exempted themselves from data breach laws that cover data held in the private sector.

---

217. 5 U.S.C. § 552a(g)(4) (2006).

218. 540 U.S. 614, 617-18, 622-23 (2004) (rejecting tort-like 'general damages').

219. The government had not contested this allegation at trial before the magistrate judge. Doe v. Herman, No. Civ. A. 297CV00043, 1999 WL 1000212, at *2 (W.D. Va. Oct. 29, 1999) (report and recommendation of magistrate judge), *report and recommendation adopted in part by* Doe v. Herman, No. Civ. A. 2:97CV00043, 2000 WL 34204432 (W.D. Va. Jul 24, 2000), *aff'd in part, rev'd in part by* Doe v. Chao, 306 F.3d 170 (4th Cir. 2002), *aff'd* by Doe v. Chao, 540 U.S. 614 (2004).

220. "The Plaintiffs allege that the distribution of this information to complete strangers has had adverse effects on them. They assert that the Department's conduct raises a serious and grave threat to privacy, security, credit ratings, identity and well-being." *Id.*

221. FLA. STAT. § 817.5681 (West 2009).

222. FLA. STAT. § 817.5681(1)(d) (West 2009); *see* Garcia, *supra* note 3, at 706.

The Federal Information Security Management Act and new federal regulations, however, require federal agencies to make serious efforts to protect private data. Major data breaches trigger a duty to disclose, at least eventually. But the administrative remedies available to parties whose data has been exposed are still paltry, generally limited to credit monitoring. Other statutes, such as the Privacy Act and the Computer Fraud and Abuse Act, create potential remedies, but, so far, only for parties who can show substantial actual (rather than feared or potential) damage.

At present, states generally lag behind the federal government both in their commitment to rigorously and systematically securing data, and in the remedies available under statute. Among the better policies needed are:

- more systematic reporting of government data breaches;
- some consistent definitions of covered data;
- enactment of statutes (state or federal) that provide for Privacy Act-like remedies against states; and
- better legal treatment of the risks of identity theft and other dangers that are triggered by a data breach. This should include those that may not be categorized as "actual injury" as required under current law.

Although there has been significant progress in some states and at the federal level, much remains to be done to improve government responses to data breaches and especially to provide remedies to those harmed by data breaches. I have argued above that a constitutional remedy combining *Whalen*, *DeShaney*, and section 1983 is available against states guilty of data breaches, at least in cases where the state failed to exercise due care when holding the data. This right is separate from any informational privacy rights that constrain the government's ability to acquire personal or corporate information. But even if courts accept this analysis, much remains to be done.