

## Articles

### A Dearth of Remedies

Elizabeth D. De Armond\*

*Federal privacy statutes purport to solidify norms for the privacy of our personal information, whether financial, medical, or other. They impose burdens on those who have control over such information. However, they often fail to offer real remedies when those burdens are not met. As a consequence, individuals may falsely perceive that the disclosure of their private data will be punished, while the regulated receive comfort that they can breach privacy with impunity. This trend of toothlessness in federal privacy law began with the Fair Credit Reporting Act, which allows some, but not complete, private remedies, and has continued through the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act. Most recently, the trend appears in congressional bills offered to protect the security of personal information, bills that prohibit private remedies and preempt such remedies that otherwise exist in state laws.*

*However, given the importance of privacy norms and the tradition of rights and remedies for privacy at the state level, states should seek to push their capacities to use laws, whether common or enacted, to protect their citizens to the very limits they can. Enforcement of social privacy*

---

\* Assistant Professor of Law, Legal Research and Writing, Chicago-Kent College of Law.

*norms, as embodied in laws state or federal, is necessary to protect personality and dignity. States can resume their traditional roles as protectors of their citizens by responding to increased threats to privacy through adapting common law torts or by enacting legislation; where these instruments provide enforcement through private causes of action, those protected by the instruments can vindicate their rights. More importantly, such remedies can deter violations to begin with, the ultimate aim of any privacy provision.*

2008]

A DEARTH OF REMEDIES

3

INTRODUCTION .....	4
I. A MODERN TREND OF REMEDILESS FEDERAL PRIVACY RIGHTS .....	5
A. <i>Privacy Laws with Curtailed Remedies</i> .....	6
1. The Fair Credit Reporting Act and Recent Amendments .....	6
a. The Original Act.....	6
b. The 1996 Amendments .....	9
c. The Fair and Accurate Credit Transactions Act of 2003.....	11
2. The Health Insurance Portability and Accountability Act 14	
3. The Gramm-Leach-Bliley Act .....	16
4. Proposed Personal Information Security Legislation.....	19
B. <i>Privacy, Personhood, and Dignity—Why Privacy Matters</i> .....	22
C. <i>Inadequate Agency Enforcement and the Impact of Rights without Remedies on Dignity and Privacy</i> .....	26
1. Problems of Administrative Enforcement.....	26
2. The Impact of Remediless Federal Privacy Rights. ....	31
II. THE TRADITION OF RIGHTS AND REMEDIES—FEDERALISM AND ENFORCEMENT .....	35
A. <i>The Tradition of State Torts</i> .....	35
B. <i>State Privacy Protection</i> .....	39
1. State Privacy Protection through Common Law Torts ...	39
2. State Protection of Privacy through Enacted Laws.....	42
C. <i>Federal Laws and the Tradition of Private Attorneys General</i> .....	45
III. A RETURN TO STATE ENFORCEMENT .....	47
A. <i>State Tort Law</i> .....	49
B. <i>State Enacted Legislation</i> .....	50
CONCLUSION.....	52

## INTRODUCTION

If a privacy right is violated, but a federal law denies the injured any remedy, has privacy been protected? Congress's interest in privacy issues has grown over the last four decades, but effective protection has shrunk. The federal government has started to regulate commercial entities' use of personal information by enacting its own statutory schemes in the area, which had previously been the province of state law. Key among these federal enactments are the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act. These federal statutes appear to protect privacy by setting standards that restrict others' use of personal information. Nonetheless, these statutes fail to fulfill their promise of privacy.

Traditionally, tort law has protected individuals from the wrongful acts of others.<sup>1</sup> Traditionally states, rather than the federal government, have adopted and developed torts and administered their remedies. Where needed to protect consumers, states have enacted legislation to augment traditional torts. While in theory no harm arises from the federal government joining the states in the business of privacy protection, federal statutes have been miserly with remedies, often providing individuals with no ability to enforce privacy provisions. In some cases, federal privacy law provisions wholly preempt state laws that would otherwise provide injured plaintiffs with a remedy, foreclosing the possibility of *any* meaningful relief for those invasions of privacy that the enactment prohibits.

Federal privacy legislation may also generate publicity that may distract individuals from the lack of enforcement power, leading them to believe they have more solid protection than in fact the federal statutes provide. This could in turn lead individuals to fail to take their own steps to protect themselves, acting under the false impression that the laws will encourage those regulated by them to comply with the laws' restrictions.

Congress is now threatening to continue this trend in its consideration of a national personal information security law.<sup>2</sup> This legislation would require those who possess sensitive consumer information to alert consumers when they learn that someone has broken through security to filch the information. The majority of states have already passed legislation that addresses this need, a need driven by advancements in database technology and the related rise of identity theft. Furthermore, several of the states that have passed such legislation

---

1. T. COOLEY, LAW OF TORTS 2-3 (1880).

2. See note 92, *infra*.

provide private remedies to those whose information has been put at risk. Nonetheless, bills pending in Congress would not only bar private remedies, but would preempt state laws that provide such remedies.<sup>3</sup> In effect, such a bill would eliminate those privacy protections from the state domain, effectively bar any injured individual from obtaining redress, and relieve business entities from the risks of treating personal information carelessly.

By eliminating remedies, these measures of the federal government collectively indicate a trend of reducing, rather than expanding, privacy rights, a trend obscured by the activity of legislating privacy “rights.” When federal measures effectively reverse states’ efforts to protect the privacy of their citizens without providing any substitute remedies, federal legislation that superficially purports to protect privacy may actually diminish it.

#### I. A MODERN TREND OF REMEDILESS FEDERAL PRIVACY RIGHTS

Privacy of personal information has drawn the attention of Congress over the last few decades. Discussed below are congressional civil acts that regulate the disclosure of information collected by non-governmental entities. Laws directed only at the collection and disclosure of individual information by governmental entities, such as the Privacy Act<sup>4</sup> and the Freedom of Information Act,<sup>5</sup> are excluded. The acts described have in common standards for privacy of personal information, but one or more handicaps in enforcement. These handicaps can undermine the desired goal of privacy laws, which is to deter breaches of privacy. Once privacy is breached, it cannot be restored, particularly in the digital age, where items of information can become immortal: genies un-bottled. Thus, to meaningfully protect privacy, laws should inhibit the initial invasion of privacy. A significant means of doing so is to put in place remedies that will motivate actors to respect the privacy of those for whom the laws exist.

---

3. See text accompanying notes 91-95, *infra*.

4. 5 U.S.C. § 552a (2006).

5. *Id.* § 552.

A. *Privacy Laws with Curtailed Remedies*

1. *The Fair Credit Reporting Act and Recent Amendments*

a. *The Original Act*

Individuals' transactions with third parties are of intense interest to lenders, businesses, employers, insurers, and marketers, among others. This thirst for information, along with accelerating developments in database technology, led consumer reporting agencies to amass huge amounts of data about Americans' personal financial matters, including their loans, bills, insurance, and employment. Alarmed by increased access to personal information, Congress passed the original Fair Credit Reporting Act (the "FCRA" or "Act") in 1970, in part to protect the privacy of consumers' transaction data.<sup>6</sup>

Congress understood how the computerization of personal information estranged individuals from their personal information, leading to a loss of control over data.<sup>7</sup> Congress sought to protect personal privacy by restricting those who could access a particular individual's financial information from a consumer reporting agency.<sup>8</sup> To gain such access, an agency's subscriber, the user of the credit report, has to certify to the agency that it has a "permissible purpose" for acquiring the information.<sup>9</sup> For the most part, the FCRA limits permissible purposes to specified needs for credit, employment, and insurance investigations.<sup>10</sup> Those who merely want to be nosy and delve through an individual's financial information are not legally able to obtain it from consumer reporting agencies. For example, the Act does not permit one who simply seeks information in connection with a lawsuit against another to obtain such information.<sup>11</sup> Furthermore, an agency may not reveal one's financial history to a party who takes an interest in the information in order to make a decision about someone else, because the Act forbids a user from obtaining a consumer report on

---

6. See Pub. L. No. 91-508 (Oct. 26, 1970) (codified as amended at 15 U.S.C. §§ 1681-1681x (2006)).

7. See 15 U.S.C. § 1681(a).

8. See 15 U.S.C. § 1681b(a).

9. 15 U.S.C. §§ 1681b(f), 1681e.

10. *Id.* § 1681b(a)(3). Governmental entities, such as child support agencies, courts, and certain regulatory agencies may also obtain consumer reports in certain circumstances. See *id.* §§ 1681b(a)(1), 1681b(a)(4), 1681b(a)(5), 1681b(a)(6).

11. See, e.g., *Bakker v. McKinnon*, 152 F.3d 1007, 1012 (8th Cir. 1998); *Duncan v. Handmaker*, 149 F.3d 424, 426-28 (6th Cir. 1998).

one person in order to judge another.<sup>12</sup> For example, an employer trying to decide whether to hire a man may not pull the credit file of the man's wife, regardless of how relevant that user thinks the history is to the hiring decision.

The Act also protects privacy by drawing a curtain on the earlier stages of one's transactional life. Agencies must exclude stale, obsolete information from a report on an individual.<sup>13</sup> For example, most information that is more than seven years old falls outside the boundaries for permissible report content.<sup>14</sup>

In addition, the Act protects privacy by prohibiting agencies from circulating damaging falsehoods about individuals to others. It does so by requiring agencies to use "reasonable procedures to assure maximum possible accuracy" of the information they put into individuals' reports.<sup>15</sup> Furthermore, once agencies learn that their files may contain inaccurate information, they must recheck the information by asking the original furnisher to verify it.<sup>16</sup>

All of these are valuable provisions that enhance personal privacy. However, although the Act was a significant step forward in federalizing privacy rights for individuals' financial information, it came at a great cost to other potential sources of privacy protection. First, the Act specifically immunizes information furnishers, users, and consumer reporting agencies from state tort suits "in the nature of defamation, invasion of privacy, or negligence" where the suits are based on information disclosed by such party pursuant to the Act.<sup>17</sup> Thus, the Act significantly undercuts a state's ability to use the threat of tort liability to discourage these parties from invading an individual's privacy, even though the FCRA may specifically prohibit the very behavior at issue. This immunity arose as a *quid pro quo* for the right of consumers to view their own information that the consumer reporting agencies had collected about them.<sup>18</sup> To override the immunity, a consumer must show that the party acted either willfully or with actual malice;<sup>19</sup> this *New York Times*

---

12. See *Zamora v. Valley Fed. Savings & Loan Ass'n*, 811 F.2d 1368, 1370 (10th Cir. 1987).

13. 15 U.S.C. § 1681c.

14. *Id.* § 1681c(a). The Act exempts some categories of information from the obsolescence rule. *Id.* § 1681c(b).

15. *Id.* § 1681e(b).

16. *Id.* § 1681i.

17. *Id.* § 1681h(e).

18. 115 CONG. REC. 33411 (1969) ("That is the quid pro quo.").

19. 15 U.S.C. § 1681h(e).

*v. Sullivan* level of malfeasance has been difficult for ordinary consumers to meet.<sup>20</sup>

The loss of state tort actions would be trivial if the federal act itself supplied sufficient remedies for infractions of privacy and effectively substituted for the lost tort remedies. Congress could have compensated for the FCRA's shield of state tort immunity for FCRA-prohibited acts by offering comparable remedies under the FCRA. Instead, though the FCRA has two civil liability provisions, as enacted these remedies provide an unsatisfactory substitute for state tort remedies. First, as a general rule, where an agency or user negligently breaches the Act, the injured party may sue for actual damages.<sup>21</sup> However, only those damages that the injured can show arose directly from the defendant's violation of the specified FCRA standard are eligible for compensation.<sup>22</sup> Injury from a disclosure permitted by the Act that may nonetheless create an actionable wrong under state tort law will fall outside the permitted compensation, but may fall inside the Act's immunity provision, protecting the wrongdoer from state law damages.<sup>23</sup> The Act also allows an individual who cannot demonstrate compensable injuries to recover nominal statutory damages, capped at \$1,000, though only where the individual can show that the agency "willfully" violated the Act.<sup>24</sup>

---

20. 376 U.S. 254 (1964). *See, e.g.*, *Morris v. Equifax Info. Servs., L.L.C.*, 457 F.3d 460, 471-72 (5th Cir. 2006) (affirming summary judgment for the defendant, a consumer reporting agency, on the plaintiff's libel claim); *Cousin v. Trans Union Corp.*, 246 F.3d 359, 374 (5th Cir. 2001) (vacating a judgment for the plaintiff on his defamation claim); *Rhodes v. Ford Motor Credit Co.*, 951 F.2d 905, 907 (8th Cir. 1991) (affirming summary judgment for the defendant, a furnisher, on the plaintiff's defamation and negligence claims); *Thurman v. Case Credit Corp.*, No. 1:04CV00003LMB, 2005 WL 3074149, at \*6 (E.D. Mo. Nov. 16, 2005) (granting summary judgment to the defendant, a furnisher, on the plaintiff's defamation claim); *Gohman v. Equifax Info. Servs., L.L.C.*, 395 F. Supp. 2d 822, 829 (D. Minn. 2005) (granting summary judgment to the defendant, a consumer reporting agency, on the plaintiff's claims for credit defamation and tortious interference with credit expectancy); *Anderson v. Trans Union, L.L.C.*, 345 F. Supp. 2d 963, 973-74 (D. Wis. 2004) (granting summary judgment to one of the defendants, a consumer reporting agency, on the plaintiff's claims for credit defamation and tortious interference with credit expectancy).

21. 15 U.S.C. § 1681o (2006). One scholar has proposed that a strict liability standard for FCRA violations would reallocate losses caused by identity theft from victims to furnishers and consumer reporting agencies, thereby providing them with a greater incentive to prevent such theft. *See* Jeff Govern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 391-93 (2003).

22. *Id.* § 1681o.

23. *Id.* § 1681h(e).

24. *Id.* § 1681n(a)(1)(A). The Supreme Court has recently ruled that a defendant's reckless disregard for the plaintiff's rights under the Act can satisfy this standard, rejecting the argument that the plaintiff must prove intent. *Safeco Ins. Co. of Am. v. Burr*, \_\_\_ U.S. \_\_\_, 127 S. Ct. 2201, 2209-10 (2007). Punitive damages are also

The second provision permits an individual to seek punitive damages, a remedy characteristic of traditional tort law, but again, only where the plaintiff can show willfulness.<sup>25</sup> However, as with the immunity provision mentioned above, willfulness has proven to be a difficult standard for individuals to meet.<sup>26</sup> Thus, while providing some opportunity for relief, the FCRA's original provisions actually narrowed, rather than expanded or even equaled, the scope of potential liability for breaching an individual's privacy.<sup>27</sup> The Act's civil liability provisions do not adequately replace the torts from which it immunizes wrongdoers.

b. The 1996 Amendments

The FCRA, as originally passed, provides wrongdoers with immunity, albeit qualified, from state torts and limits their exposure to punitive damages. Congress has retained this immunity through various revisions of the Act and, in 1996, expanded the pool of those who could claim the benefits of the immunity provision's shield. Among the actors that may claim the protections of this provision are those who furnish information about individuals and their transactions to consumer reporting agencies. Typically, these are parties with which an individual dealt with directly, perhaps without realizing that the information given might someday make it to a wider audience.

Originally, the FCRA did little to control furnishers of information. Furnishers are the banks, credit card issuers, utilities, insurers and others that give personal information about their customers to consumer reporting agencies, to be pooled with information from other furnishers and then delivered to those who request reports about those customers.

---

permitted where a user obtains a consumer report under false pretenses or knowingly without a permissible purpose. 15 U.S.C. § 1681n(b).

25. 15 U.S.C. § 1681n(a)(2).

26. *See, e.g., Casella v. Equifax Credit Info. Servs.*, 56 F.3d 469, 486 (2d Cir. 1995) (affirming summary judgment for the defendant, a consumer reporting agency, reasoning that the plaintiff had failed to show sufficient evidence that the agency's failure to delete inaccurate information was willful), *cert. denied*, 517 U.S. 1150 (1996); *Stevenson v. TRW, Inc.*, 987 F.2d 288, 294 (5th Cir. 1993) (ruling that the trial court's finding of willfulness was clearly erroneous); *Pinner v. Schmidt*, 805 F.2d 1258, 1263 (5th Cir. 1986) (vacating a jury's award of punitive damages against a consumer reporting agency). The Eighth Circuit requires "knowing and intentional commission of an act the defendant knows to violate the law." *Phillips v. Grendahl*, 312 F.3d 357, 370 (8th Cir. 2002).

27. Generally, an action for invasion of privacy can yield damages both for monetary harm and mental distress, including "emotional distress or personal humiliation." RESTATEMENT (SECOND) OF TORTS § 652H, 652H cmt. b (1979). Some jurisdictions permit additional damages. *See, e.g., Shahi v. Madden*, 949 A.2d 1022, 1034-35 (Vt. 2008) (affirming punitive damages award of \$1,000,000 on invasion of privacy claim); *Pearson v. Kancilia*, 70 P.3d 594, 599 (Colo. Ct. App. 2003) (affirming punitive damage award of \$200,000 on intrusion upon seclusion claim).

However, in 1996, Congress extended the Act to impose responsibilities on those who furnish individuals' financial transaction information to agencies.<sup>28</sup> On their face, the 1996 provisions appeared to significantly advance the interests of individuals by requiring furnishers to refrain from knowingly reporting false information, and to correct and update information, among other duties of care.<sup>29</sup> In theory, this provision could curb furnishers who might damage consumers' financial reputations by carelessly reporting false information about their transactions. These provisions could have significantly enhanced privacy by imposing, for the first time, a federal duty of care in the disclosure of personal transaction information to consumer reporting agencies.

Congress, however, retained the Act's qualified immunity provision for furnishers and expanded the provision's reach, immunizing furnishers from state actions for invasion of privacy, defamation, and negligence that an individual could have otherwise pursued under state common or statutory law.<sup>30</sup> Had Congress not done so, the standards set by the provisions could have had meaning in a state action. For example, an FCRA provision could have served as the statutory standard in a negligence *per se* action.<sup>31</sup> Thus, what appeared to advance the privacy rights of individuals by federalizing obligations of furnishers actually curtailed the ability of individuals to protect themselves.

Congress went even further in favor of furnishers. Though individuals may still usually pursue consumer reporting agencies through the Act itself when such agencies violate their obligations, Congress specifically shielded furnishers from the risk of liability under the Act for some of the most egregious violations of their new obligations. It provided that the Act's civil liability provisions did not apply to violations of all but one of the new duties.<sup>32</sup> Perhaps the most important of the new duties, that prohibiting furnishers from providing information that the furnisher knew or should have known to be false,<sup>33</sup> cannot be the subject of a private cause of action. Accordingly, an individual who has been injured by a furnisher's breach of these new responsibilities under

---

28. Pub. L. No. 104-208, § 2413 (Sept. 30, 1996).

29. 15 U.S.C. § 1681s-2(a) (2007).

30. Pub. L. No. 104-208 § 2408(e)(4).

31. See *Martin v. Herzog*, 126 N.E. 814, 815 (N.Y. 1920); RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL HARM § 14 (Proposed Final Draft 2006); see also *Moody v. Experian Info. Solutions, Inc.*, 57 Fed. Appx. 211, 2003 WL 147741, at \*1 (5th Cir. 2003) (ruling that the FCRA's qualified immunity provision applied to a negligence *per se* action based on the defendant's alleged breach of the Act's standards); Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 264 (2005) (discussing how state information security statutes may give rise to a cause of action even though they do not expressly create such a cause of action).

32. 15 U.S.C. § 1681s-2(c).

33. *Id.* § 1681s-2(a)(1).

the Act would, in most cases, have to hope that the designated federal or state authorities would come to the individual's defense and bring suit against the violating furnisher on the individual's behalf.<sup>34</sup> The individual could not, on his or her own, seek compensation for the misuse of personal information. The sole duty left open for private remedies is that requiring a furnisher to reinvestigate the accuracy of an item that a consumer has disputed, and this duty only arises when the furnisher has received notice of the dispute from a consumer reporting agency.<sup>35</sup>

That Congress eliminated any liability under the Act for many furnisher violations alone would have disarmed individuals who suffered violations of the Act. However, Congress was not satisfied that the qualified immunity provision that protected those regulated by the Act from tort liability, along with the elimination of a private remedy through the Act, would sufficiently shield feckless furnishers from having to compensate anyone for their wrongdoing. Accordingly, Congress specifically preempted states from protecting their consumers from privacy invasions that pertained in any way to the subject matter of the new federal protections from furnishers.<sup>36</sup> By doing so, Congress hamstrung the ability of states to protect consumers from furnishers who provide false, inaccurate, or obsolete information to agencies, and also severely impaired the abilities of consumers to enforce the substance of the new obligations.

Effectively, then, most of the newly enacted rights existed on paper only, and states lost a great deal of power. The lesson for furnishers of information was that they could breach the Act's privacy standards with impunity. Accordingly, what appeared to be new privacy rights turned out to be a muted license to traffic in personal information. This preemption, however, was not intended to be permanent. The crippling of state authority was originally due to expire January 1, 2004.<sup>37</sup>

c. The Fair and Accurate Credit Transactions Act of 2003

Congress rolled back individual privacy remedies even further in 2003, when it passed the Fair and Accurate Credit Transactions Act ("FACTA"), amending the FCRA. FACTA stripped some existing claims, expanded the list of provisions for which no private claims may

---

34. *See id.* § 1681s (identifying governmental authorities authorized to enforce the Act).

35. *Id.* §§ 1681s-2(b), 1681s-2(c)(1).

36. Pub. L. No. 104-208, §§ 2413, 2419 (Sept. 30, 1996) (codified as amended at 15 U.S.C. § 1681t).

37. *Id.* § 2419.

be brought, and both expanded and solidified the FCRA's preemption of state laws.<sup>38</sup>

Until that time, some significant privacy protections that consumers could claim were the Act's requirements of users that take action based on information in a consumer report. The FCRA requires a user that takes an action adverse to a consumer to notify the consumer that the action was based at least in part on a consumer report and to identify the agency that issued the report.<sup>39</sup> A user has to provide a consumer with this adverse action notice whenever information in a consumer's report led the user, for example, to deny or revoke credit or insurance, or raise charges or premiums, or fire or refuse to hire someone.<sup>40</sup> In addition, the FCRA requires creditors to notify their customers when they deny or increase a credit charge based on information that they receive from a source other than a consumer reporting agency.<sup>41</sup> These rights enhance individuals' privacy by alerting them to the use of their private financial information and by warning them that negative information about them is not only held in the hands of a consumer reporting agency or another, but is being disclosed to third parties as well.

From the FCRA's inception, consumers could enforce these protections through a private action under the Act.<sup>42</sup> However, in a stunning strike against individual privacy, Congress eliminated the decades-old enforcement right by prohibiting nearly all causes of action by consumers against users of consumer reports who violate the Act's requirements.<sup>43</sup>

---

38. Pub. L. No. 108-159 (Dec. 4, 2003).

39. 15 U.S.C. § 1681m(a).

40. *Id.* §§ 1681a(k), 1681d(a)(6).

41. *Id.* § 1681m(b). This notice requirement applies to denials of credit for personal, family, or household purposes where the information bears on the consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, but does not apply to denials of insurance or employment. *Id.*

42. *Id.* §§ 1681n, 1681o.

43. *Id.* § 1681m(h)(8); *see also* Bonner v. CorTrust Bank, N.A., No. 2:05-CV-137 PS, 2006 WL 1980183, at \*\*3-4 (N.D. Ind. July 12, 2006); Miller v. CoreStar Fin. Group of Pa., Inc., No. 05-5133, 2006 WL 1876584, at \*\*2-3 (E.D. Pa. June 29, 2006); Crowder v. PMI Mortg. Ins. Co., No. 2:06CV0114-VPM, 2006 WL 1528608, at \*4 (M.D. Ala. May 26, 2006) (rejecting argument that section 1681m(h)(8) should not be applied retroactively); Bonner v. Home123 Corp., No. 2:05-CV-146 PS, 2006 WL 1518974, at \*4 (N.D. Ind. May 25, 2006); Bruce v. Wells Fargo Bank, N.A., 2006 WL 1195210, at \*2 (N.D. May 2, 2006); Bruce v. Grieger's Motor Sales, Inc., 422 F. Supp. 2d 988, 991 (N.D. Ind. 2006); Putkowski v. Irwin Home Equity Corp., No. C 05-3289 PJH, 2006 WL 741387, at \*8 (N.D. Cal. Mar. 23, 2006); Bonner v. H & R Block Mortg. Corp., No. 2:05-CV-162, 2006 WL 760258, at \*3 (N.D. Ind. Mar. 23, 2006); Phillips v. New Century Fin. Corp., No. SACV050692DOCRNBX, 2006 WL 517653, at \*\*2-4 (C.D. Cal., Mar. 1, 2006); Harris v. Fletcher Chrysler Prods., Inc., No. 1:05-CV-1140-LJM-VSS, 2006 WL 279030, at \*2 (S.D. Ind. Feb. 2, 2006); White v. E-Loan, Inc., 409

Congress not only eliminated the cause of action, but it simultaneously retained the explicit preemption of state laws that could protect consumers from over-aggressive users.<sup>44</sup> In fact, Congress made permanent *all* of the preemption provisions of the 1996 legislation that were originally intended to be temporary, and were due to sunset the first day of 2004.<sup>45</sup> That the limitations on the ability of states to regulate furnishers of information were about to sunset led to widespread panic among industry participants who traffic in consumers' personal information and was a major impetus for the 2003 legislation.<sup>46</sup> To satisfy these participants, Congress solidified the preexisting preemption provisions and added a batch of additional preemption provisions, further weakening the states' ability to offer the remedies to consumers that Congress had denied to them.<sup>47</sup> Industry participants have since

---

F. Supp. 2d 1183, 1184-87 (N.D. Cal. 2006); Killingsworth v. Household Bank (SB), N.A., No. 05 C 5729, 2006 WL 250704, at \*3 (N.D. Ill. Jan. 31, 2006); Stavroff v. Gurley Leep Dodge, Inc., No. 3:05 CV 229, 2006 WL 196381, at \*\*2-5 (N.D. Ind. Jan. 20, 2006); Villagran v. Freeway Ford, Ltd., No. Civ.A. H-05-2687, 2006 WL 964731, at \*1 (S.D. Tex. Jan. 19, 2006); Murray v. Cross Country Bank, 399 F. Supp. 2d 843, 844 (N.D. Ill. 2005); Murray v. Household Bank (SB), N.A., 386 F. Supp. 2d 993, 997-99 (N.D. Ill. 2005); Hernandez v. Citifinancial Servs., Inc., No. 05 C 2263, 2005 WL 3430858, at \*6 (N.D. Ill. Dec. 9, 2005); McCane v. America's Credit Jewelers, Inc., No. Civ.A. 05 C 5089, 2005 WL 3299371, at \*3 (N.D. Ill. Dec. 1, 2005); Phillips v. New Century Fin. Corp., No. SACV05-0692DOC(RNBX), 2005 WL 3828735, at \*5, (C.D. Cal. Nov. 9, 2005); Pietras v. Curfin Oldsmobile, Inc., No. Civ.A. 05 C 4624, 2005 WL 2897386, at \* 4 (N.D. Ill. Nov. 1, 2005). *But see* Barnette v. Brook Road, Inc., 429 F. Supp. 2d 741, 749 (E.D. Va. 2006) (holding that amendment did not eliminate private cause of action for all subsections of 15 U.S.C. § 1681m).

44. 15 U.S.C. § 1681t(b)(1)(C) (preempting as to § 1681m(a) and (b), relating to users' adverse actions against individuals); *id.* § 1681t(b)(1)(D) (preempting as to § 1681m(d), relating to users' use of consumer reports in connection with making a firm offer of credit or insurance); *id.* § 1681t(b)(1)(I) (preempting as to § 1681m(h), relating to the use of credit reports in risk-based-pricing); *id.* § 1681t(b)(5)(F) (preempting as to §§ 1681m(e), (f), and (g), measures concerning identity theft).

45. *Id.* § 1681t(d).

46. *Id.* § 1681t(d). *See* EVAN HENDRICKS, CREDIT SCORES & CREDIT REPORTS: HOW THE SYSTEM REALLY WORKS, WHAT YOU CAN DO 337-65 (2d ed. 2005) (describing the behind-the-scenes activities leading up to the passage of FACTA).

47. Pub. L. No. 108-159, § 151(a)(2) (preempting state laws relating to certain information to be made available to identity theft victims); Pub. L. No. 108-159, § 214(c)(2) (preempting state laws relating to the sharing of information by affiliates for marketing purposes); Pub. L. No. 108-159, § 212(e) (preempting state law with respect to designated disclosures agencies are to make); Pub. L. No. 108-159, § 311(b) (preempting state laws with respect to risk-based credit pricing notices); Pub. L. No. 108-159, § 711 (preempting state laws with respect to requirements for the truncation of credit card and debit card numbers, identity theft fraud alerts, blocking of information resulting from identity theft, social security number digit exclusion from credit reports, free annual credit reports, red flag guidelines, prohibition on sale or transfer of debt caused by identity theft, debt collector communications concerning identity theft, coordination of consumer complaint investigations among agencies, duties of furnishers upon notice of identity theft-related information, and disposal of records).

effectively used the provisions to invalidate state efforts to address information privacy concerns.<sup>48</sup>

In sum, the FCRA establishes federal standards to limit the use and disclosure of certain personal information related to individuals' financial transactions. However, Congress has increasingly weakened the ability of consumers to enforce these protections, whether at the federal or the state level. The original Act granted regulated parties a generous shield from state tort actions and limited remedies for violations. Later, Congress added to the Act requirements for furnishers, but protected such data disclosers from the private enforcement mechanisms that Congress incorporated into the Act, and temporarily preempted state laws regulating much of the subject matter of the 1996 additions. In 2003, Congress via FACTA solidified preemption provisions that were intended to be temporary, added new provisions that similarly quelled state law, and eliminated wholesale any private cause of action for a whole category of provisions that consumers had been able to enforce since the Act's inception.

## 2. *The Health Insurance Portability and Accountability Act*

Other federal enactments have followed up on the FCRA's model, providing the appearance of new privacy rights with the actuality of reduced privacy remedies. Both the FCRA, discussed above, and the Gramm-Leach-Bliley Act, discussed below, pertain to the privacy of individuals' financial information. Such information is sensitive because it has the power to make people feel vulnerable to the judgments of those who learn of it. Medical information, however, is also quite sensitive, and one of the most visible actions of Congress in protecting (or appearing to protect) consumers' privacy is the Health Insurance Portability and Accountability Act ("HIPAA" or the "Act"), passed in 1996.<sup>49</sup> Pursuant to that Act, the Department of Health and Human Services promulgated privacy regulations that implement the Act's privacy provisions, collectively known as the "Privacy Rule," which

---

48. *See, e.g.,* American Bankers Ass'n v. Gould, 412 F.3d 1081, 1087 (9th Cir. 2005) (holding that the FCRA's preemption of state law with respect to its provision that allows affiliates to share consumers' financial information invalidated aspects of California's sweeping financial information privacy statute); Consumer Data Industry Ass'n v. Swanson, No. 07-CV-3376, 2007 WL 2219389, at \*5 (D. Minn. July 30, 2007) (relying on FCRA's preemption provision to enjoin the state's attorney general from enforcing a newly enacted provision, Minn. Stat. § 13C.01 (2008), that prohibited consumer reporting agencies from generating lists of consumers who have applied for mortgages, known as "mortgage trigger lists," and marketing them to third parties).

49. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of titles 18, 26, 29, and 42 of the United States Code).

apply to “covered entities.”<sup>50</sup> The Privacy Rule prohibits covered entities, which include hospitals, insurers, and other participants in the medical industry, from using or disclosing protected health information, unless the use or disclosure is specifically permitted.<sup>51</sup> In promulgating the Privacy Rule, the Secretary of Health and Human Services emphasized the importance of privacy as “a fundamental right [that] must be viewed differently than any ordinary economic good.”<sup>52</sup>

HIPAA received a great deal of publicity when the Privacy Rule went into effect, coverage that emphasized the Rule’s provisions governing the disclosure of health records.<sup>53</sup> However, that coverage did not completely accord with reality. HIPAA primarily demands notices, rather than restricts disclosures. The Privacy Rule provides that a consumer “has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual’s rights and the covered entity’s legal duties with respect to protected health information.”<sup>54</sup> The Rule does require an entity to seek a consumer’s consent before disclosing information for marketing procedures.<sup>55</sup> Psychotherapy notes, perhaps the information with the most potential to humiliate, also receive special protections.<sup>56</sup> Despite the stated purpose, however, the Rule provides entities with wide latitude to use and disclose medical information to carry out treatment and health care operations.<sup>57</sup> In addition, and perhaps less justifiably, covered entities may disclose medical information, no matter how personal and individually attributable to a specific patient, in order to obtain payment.<sup>58</sup> As such, these exceptions to HIPAA weaken the purported protections.

More disturbingly, regardless of how much or how little HIPAA limits the wanton use of private medical information, covered entities

---

50. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461-82,510 (Dec. 28, 2000).

51. 45 C.F.R. § 164.502(a).

52. 65 Fed. Reg. 82,462, 82,464-82,465 (Dec. 28, 2000), available at <http://aspe.hhs.gov/admsimp/>. The Secretary also acknowledged that state tort law is a primary protector of privacy interests. *Id.* at 82464.

53. See, e.g., Sandra G. Boodman, *Privacy, Please; New Rules May Protect Patients, Alter Hospital, Office Practices*, WASH. POST, Apr. 8, 2003, at F01; Martin Miller, *A Tougher Medical Privacy Law; Health Care Providers Are Hurrying to Comply With a Federal Law that Aims to Further Limit the Spread of Patient Information*, L.A. TIMES, Apr. 14, 2003, at part 6, 1; Robert Pear, *Health System Warily Prepares for New Privacy Rules*, N.Y. TIMES, Apr. 6, 2003, at A1.

54. 45 C.F.R. § 164.520.

55. *Id.* § 164.508(a)(3)(i).

56. *Id.* § 164.508(a)(2)(i).

57. *Id.* § 164.506(c)(1).

58. *Id.*

remain free from fear that any individual injured by a violation of HIPAA will be able to enforce any rights under the Act. HIPAA provides for administrative enforcement, but does not specifically provide that injured individuals may sue to recover for violations. Every court to examine the issue has held that Congress did not intend to allow individuals to enforce their rights under the Act, but rather intended only that administrative agencies be permitted to enforce the law.<sup>59</sup> The tepidity of such enforcement is described later on in this article.<sup>60</sup>

However, in contrast to the FCRA, with its multiple preemption provisions,<sup>61</sup> HIPAA does not throw states out of the privacy protection arena. In fact, state law controls where it provides more stringent protection for individually identifiable health information.<sup>62</sup>

### 3. *The Gramm-Leach-Bliley Act*

After HIPAA, Title V of the 1999 Gramm-Leach-Bliley Act (“GLB” or the “Act”) became the next significant consumer privacy legislation that Congress passed.<sup>63</sup> Provisions in GLB appear to protect privacy by restricting financial institutions’ use of certain consumer

---

59. Courts have consistently ruled that HIPAA does not provide for an implied private cause of action. *See, e.g.,* *Acara v. Banks*, 470 F.3d 569, 572 (5th Cir. 2006); *Cain v. Mitchell*, No. 06-00897-CV-W-FJG, 2007 WL 4287866, at \*2 (W.D. Mo. Dec. 6, 2007); *Fast v. Fast*, No. 8:07CV310, 2007 WL 2417384, at \*2 (D. Neb. Aug. 23, 2007); *Valentin Munoz v. Island Fin. Corp.*, 364 F. Supp. 2d 131, 136 (D.P.R. 2005); *Johnson v. Parker Hughes Clinics*, No. Civ.04-4130 PAM/RLE, 2005 WL 102968, at \*2 (D. Minn. Jan. 13, 2005); *Univ. of Colo. Hosp. v. Denver Publ’g Co.*, 340 F. Supp. 2d 1142, 1144-45 (D. Colo. 2004); *Logan v. Dept. of Veterans Affairs*, No. 02-701 (RJL), 2004 WL 3168183, at \*4 (D.D.C. July 28, 2004); *Ass’n of Am. Physicians & Surgeons, Inc. v. U.S. Dept. of Health & Human Servs.*, 224 F. Supp. 2d 1115, 1129 (S.D. Tex. 2002); *O’Donnell v. Blue Cross Blue Shield of Wyo.*, 173 F. Supp. 2d 1176, 1180 (D. Wyo. 2001).

60. *See* text accompanying notes 136 to 143, *infra*.

61. *See* text accompanying notes 45 to 48, *supra*.

62. 45 C.F.R. § 160.203(b) (2006). The regulation identifies other exceptions to preemption as well. *Id.* For an analysis of the execution of the preemption provision, see Beverly Cohen, *Reconciling the HIPAA Privacy Rule with State Laws Regulating Ex Parte Interviews of Plaintiffs’ Treating Physicians: A Guide to Performing HIPAA Preemption Analysis*, 43 HOUS. L. REV. 1091 (2006). For a critique of these preemption provisions, see Grace Ko, Comment, *Partial Preemption Under the Health Insurance Portability and Accountability Act*, 79 S. CAL. L. REV. 497 (2006). State law is defined broadly to mean “a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.” 45 C.F.R. § 160.202.

63. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801-6809 (2006)). The Act is also known as the Financial Services Modernization Act of 1999. In addition, the Act prohibits third parties from obtaining protected information through false pretenses. 15 U.S.C. §§ 6821-27 (2006).

information.<sup>64</sup> Specifically, the Act regulates the use of “nonpublic personal information,” defined as any personally identifiable financial information that the consumer provides to the institution, that results from any transaction with the consumer or service the institution performs for the consumer, or that the institution otherwise obtains.<sup>65</sup>

The Federal Trade Commission issued its Financial Privacy Rule to implement certain details of GLB;<sup>66</sup> this Rule is distinct from HIPAA’s Privacy Rule.<sup>67</sup> The Rule provides examples of personally identifiable financial information that include the simple fact that an individual was a customer, account balance information, and data that an individual provides on an account application.<sup>68</sup> The definition specifically excludes any “publicly available information” from the protected class of information.<sup>69</sup>

As a general matter, GLB promotes privacy by prohibiting a financial institution from disclosing nonpublic personal information about a consumer to a third party unless the institution has provided the

---

64. The Act defines “financial institution” to include any institution the business of which is engaging in financial activities as described in § 1843(k) of Title 12. 15 U.S.C. § 6809(3).

65. See 15 U.S.C. § 6809(4). The FTC’s definition of “personally identifiable financial information” has been upheld against a challenge that the FTC exceeded its authority in defining the term. See *Trans Union LLC v. F.T.C.*, 295 F.3d 42, 50-51 (D.C. Cir. 2002). GLB also requires agencies subject to the Act to establish standards “relating to administrative, technical and physical safeguards” to ensure the security of records. 15 U.S.C. § 6801(b). To implement this provision, the FTC issued the “Safeguards Rule,” which requires financial institutions within the FTC’s jurisdiction to develop and maintain an information security program that contains certain designated elements. 16 C.F.R. pt. 313 (2006). The other agencies subject to GLB issued similar rules. 12 C.F.R. § 30 Appx. B (Office of The Comptroller of the Currency) (2005); *id.* § 208 Appendix D-2 (Federal Reserve); *id.* § 364 Appx. B (Federal Deposit Insurance Corporation); *id.* § 570 Appx. B (Office of Thrift Supervision); *id.* § 748 Appx. A (National Credit Union Administration).

66. See 16 C.F.R. pt. 313. In addition to the Federal Trade Commission, GLB specifically grants enforcement authority to the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Director of the Office of Thrift Supervision, the Board of the National Credit Union Administration, the Securities and Exchange Commission, and state insurance authorities. See 15 U.S.C. §§ 6805(a)(1)(A)-(D), 6805(a)(2)-(6). The Comptroller of the Currency’s regulations are codified at 12 C.F.R. pt. 40; the Board of Governors’ at 12 C.F.R. pt. 216; the FDIC’s at 12 C.F.R. pt. 332; the Office of Thrift Supervision’s at 12 C.F.R. pt. 573; the NCUA’s at 12 C.F.R. pt. 716; and the SEC’s at 12 C.F.R. pt. 248.

67. See text accompanying notes 50 to 52, *supra*.

68. See 16 C.F.R. § 313.3(o)(2)(i).

69. The Federal Trade Commission has defined “publicly available information” to be “any information that you have a reasonable basis to believe is lawfully made available to the general public from: (i) Federal, State, or local government records; (ii) Widely distributed media; or (iii) Disclosures to the general public that are required to be made by Federal, State, or local law.” *Id.* § 313.3(p)(1).

consumer with an initial privacy notice, has notified the consumer of the right to opt out of the disclosure, and has given the consumer a reasonable opportunity to opt out.<sup>70</sup> The institution must then await the consumer's compliance with the institution's procedures for opting out.<sup>71</sup> However, should the consumer not take that step, or fail to follow the opt-out instructions precisely, the institution then becomes free to use the consumer's information.<sup>72</sup>

Thus, GLB does not directly prohibit financial institutions from sharing customer information. Rather, the Act merely requires institutions to provide certain notices to consumers, including a notice of the consumer's right to opt out of some disclosures of personal information.<sup>73</sup> Once a consumer has passed on the opportunity to opt out, the institution may freely share that consumer's information with whomever it chooses,<sup>74</sup> a feature that led one California legislator to describe GLB as "a fig leaf."<sup>75</sup> In contrast, at common law one who discloses private information may be liable under the tort of public disclosure of private facts.<sup>76</sup> The tort does not require the injured individual to have first notified the tortfeasor that he or she did not want the information shared.<sup>77</sup>

The opt-out requirement significantly weakens the impact of GLB's privacy provisions. In addition, Congress incorporated a slew of exempt disclosures that also undermine the impact of the Act.<sup>78</sup> The most significant among the exempt disclosures are those made between affiliates; disclosures to an institution's own affiliates are completely unrestricted by GLB and its Financial Privacy Rule.<sup>79</sup>

---

70. See 15 U.S.C. § 6802(b)(1); see also 16 C.F.R. § 313.10(a)(1).

71. See 15 U.S.C. § 6802(b)(1); see also 16 C.F.R. § 313.10(a)(1).

72. See 15 U.S.C. § 6802(a).

73. See *id.* §§ 6802, 6803.

74. The Act does restrict the sharing of one particularly sensitive category of information regardless of the consumer's opt out: account numbers and similar forms of access codes. However, even that prohibition is subject to exceptions. See *id.* § 6892(d); see also 16 C.F.R. § 313.12.

75. Jennifer 8. Lee, *California Law Provides More Financial Privacy*, N.Y. TIMES, Aug. 28, 2003, at A1 (quoting Jackie Speir, a main sponsor of a California financial privacy act).

76. See W.P. KEETON, PROSSER & KEETON ON THE LAW OF TORTS 856-57 (5th ed. 1984); see also RESTATEMENT (SECOND) OF TORTS § 652D (1979); text accompanying notes 209 to 211, *infra*.

77. See RESTATEMENT (SECOND) OF TORTS § 652D.

78. See 15 U.S.C. § 6802(e)(1) (listing exempt disclosures); see also 16 C.F.R. §§ 313.4(a), 313.14-16 (same).

79. See 15 U.S.C. § 6802. The Act and the Financial Privacy Rule merely require that the institution's privacy notice disclose its policy with respect to disclosing nonpublic personal information to affiliates. See *id.* at § 6802(a)(1); see also 16 C.F.R. § 313.6.

While the privacy protections of GLB are weak, the opportunities for enforcing those protections are even weaker. The Act did not specifically provide any mechanism by which a consumer could sue to enforce its provisions.<sup>80</sup> Accordingly, every court to address the issue has dismissed individuals' suits brought pursuant to the Act, holding that Congress did not intend to provide individuals with any kind of remedy for the breaches of privacy prohibited by the Act.<sup>81</sup>

Instead of allowing people to enforce these federal privacy rights, the Act left them open to only administrative enforcement.<sup>82</sup> However, these agencies have not assertively pursued enforcement; therefore, the Act's privacy protections are largely ornamental.<sup>83</sup> To Congress's credit, however, in contrast to the sweeping preemption provisions of the FCRA, GLB does not preempt states from enacting their own privacy protections in this area,<sup>84</sup> and in this way has done less damage than the FCRA to individuals' ability to protect their privacy in state court. Accordingly, some states have themselves enacted remedies for those injured by behavior that violates GLB.<sup>85</sup>

#### 4. *Proposed Personal Information Security Legislation*

Actions in the new area of data security typify the philosophical gap between state and federal measures on matters of privacy. Recently, states have led the way in creating legislation to guard against the damage caused when the security of computerized information is breached.<sup>86</sup> California's breach statute serves as a model;<sup>87</sup> it provides

---

80. See 15 U.S.C. §§ 6801-6810.

81. See, e.g., *Farley v. Williams*, No. 02-CV-0667C(SR), 2005 WL 3579060, at \*3 (W.D.N.Y. Dec. 30, 2005); *Borinski v. Williamson*, No. Civ.A. 3:02-CV-1014-, 2004 WL 433746, at \*3 (N.D. Tex. Mar. 1, 2004) (no private cause of action under GLB); *Lacerte Software Corp. v. Prof'l Tax Servs., L.L.C.*, No. Civ.3:03-CV-1551-H, 2004 WL 180321, at \*2 (N.D. Tex. Jan. 6, 2004) (same); *Menton v. Experian Corp.*, No. 02 Civ. 4687(NRB), 2003 WL 21692820, at \*3 (S.D.N.Y. July 21, 2003) (same); see also *Dunmire v. Morgan Stanley DW, Inc.*, 475 F.3d 956, 960 (8th Cir. 2007) (stating that no private cause of action exists under GLB).

82. See 15 U.S.C. § 6805.

83. See text accompanying notes 153 to 156, *infra*.

84. See 15 U.S.C. § 6807(a). In fact, the statute explicitly provides that a more protective state law will not be preempted, so long as it does not conflict with the federal provision. *Id.* § 6807(b).

85. See, e.g. ARIZ. REV. STAT. § 20-2121 (2001) (governmental enforcement); COLO. REV. STAT. ANN. § 6-1-716 (West 2006) (relating to security breaches); IOWA CODE ANN. § 505.8 (West 2007); KAN. STAT. ANN. § 40-2404 (West 2004) (private enforcement through state Deceptive Trade Practices Act); 9-B ME. REV. STAT. ANN. § 241 (West 1997) (same).

86. See, e.g., ARIZ. REV. STAT. § 44-7501; CAL. CIV. CODE § 1798.82 (West 2007); 815 ILL. COMP. STAT. 530/1 to 530/20. For a complete list, see National Conference of State Legislatures, State Security Breach Notification Laws, <http://www.ncsl.org/>

that any business doing business in California must disclose the breach of security of computerized data that includes personal information.<sup>88</sup> The statute specifically authorizes private civil actions to enforce its security standards.<sup>89</sup> Following California's example, several states have provided that those whose personal information has been put at risk of disclosure in violation of a personal information security statute can bring a suit for damages.<sup>90</sup> State attorneys general, pursuant to state consumer fraud statutes, have also pursued institutions that have put individuals' data at risk.<sup>91</sup>

---

programs/lis/cip/priv/breachlaws.htm. See also National Conference of State Legislatures, 2006 Breach of Information Legislation, [www.ncsl.org/programs/lis/cip/priv/breach.htm](http://www.ncsl.org/programs/lis/cip/priv/breach.htm). For a discussion of the potential impact of federal preemption on such laws, see Katherine E. Picanso, Comment, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 *FORDHAM L. REV.* 355 (2006).

87. See CAL. CIV. CODE § 1798.82 (West 2008).

88. See *id.* § 1798.82(a).

89. See *id.* § 1798.84(b).

90. See, e.g., HAW. REV. STAT. § 487N-3(b) (2007) (imposing liability to injured parties); 815 ILL. COMP. STAT. 530/20 (2008) (providing that a violation constitutes an unfair trade practice); LA. REV. STAT. ANN. § 51:3075 (2008) (authorizing damages); MD. CODE, COM. LAW § 14-3508 (2008) (providing that a violation constitutes an unfair trade practice); N.J. STAT. ANN. § 56:8-166 (2008) (providing that a willful, knowing, or reckless violation constitutes an unfair trade practice); N.C. GEN. STAT. § 75-65(i) (2008) (providing for a cause of action to those injured by a violation); N.D. CENT. CODE § 51-30-07 (2007) (providing that a violation constitutes an unfair trade practice); N.H. REV. STAT. ANN. § 359-C:21 (2008) (providing for a cause of action, authorizing treble damages for willful violations); R.I. GEN. LAWS § 11-49.2-6 (2007) (civil penalties); TENN. CODE ANN. § 47-18-2107 (2008) (authorizing private cause of action); TEX. BUS. & COM. CODE § 48.203 (2007) (providing that a violation constitutes an unfair trade practice); WASH. REV. CODE § 19.225.010(10) (2008) (authorizing private cause of action); WIS. STAT. § 895.507(4) (2007) (indicating that failure to comply may be evidence of negligence or a breach of a legal duty); see also NEV. REV. STAT. §§ 603A.909, .910 (2007) (authorizing action by the data collector and providing for restitution). Several other states authorize enforcement by a public entity without specifically prohibiting private causes of action. See, e.g., ARK. CODE ANN. § 4-110-108 (2008); COLO. REV. STAT. § 6-1-716(4) (2008); CONN. GEN. STAT. ANN. § 36a-701b(g) (2008) (providing that a violation constitutes an unfair trade practice); DEL. CODE ANN. tit. 6 § 12B-104 (2008); IDAHO CODE ANN. § 28-51-107 (2008); 10 ME. REV. STAT. ANN. § 1349 (2008); MASS. GEN. LAWS. ch. 93H § 6 (2008); MINN. STAT. § 325E.61(6) (2008); N.J. STAT. ANN. § 56:8-163 (2008); N.Y. GEN. BUS. LAW § 899-aa(6) (2008); NEB. REV. STAT. § 87-806 (2007); R.I. GEN. LAWS § 11-49.2-6 (2007); VT. STAT. ANN. tit. 9, § 2435(g) (2008). Other states expressly limit enforcement to state entities. See, e.g., W.V. STAT. § 46-2A-104 (2008) (providing exclusive enforcement authority to the state's Attorney General or to a financial institution's primary functional regulator, as appropriate); see also Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 *MICH. L. REV.* 913, 972-84 (2007) (providing a chart of state data security breach laws).

91. See, e.g., *In re Eli Lilly, Inc.*, Assurance of Voluntary Compliance and Discontinuance, available at <http://www.epic.org/privacy/medical/lillyagreement.pdf>.

Recent bills in Congress purport to propose federal data security protections.<sup>92</sup> They would require entities to create programs to keep sensitive personal information secure and to notify consumers of suspected security breaches.<sup>93</sup> These bills extend the trend discussed above. On their face, the proposed bills appear to set standards that seem to favor individuals. However, two of the bills explicitly prohibit private causes of action for any violation of its provisions, no matter how egregious.<sup>94</sup> Not only may individuals not enforce the violations through the federal act, but the majority of the bills specifically squelch the effect of any state action relating to any act or practice governed under the federal act.<sup>95</sup>

Should Congress successfully enact one of these preempting bills, however, the bill would likely be perceived as a victory for individual data protection and personal privacy because it would provide a set of national standards to regulate data security breaches. In fact, however, it would roll protections back in several states where state legislatures have passed meaningful data security statutes that allow either consumers, state officials, or both to enforce the statutory standards.<sup>96</sup> Such remedies likely motivate compliance with the law in a way that will be lost if Congress passes one of the preemptive and powerless bills.

In sum, three of the marquee pieces of federal privacy legislation have features that pull the privacy punch that they could have delivered. Neither HIPAA nor GLB permit those who are injured by their breach to enforce the rights granted in the acts. This lack of private enforcement opportunities may well, as discussed below, weaken the motivation for those regulated to comply with their obligations. While the FCRA authorizes some private actions, it specifically denies them for some of the most important protections.<sup>97</sup> The FCRA further hamstringing individuals by creating a high barrier to punitive damages and by

---

92. Active bills in the 110th Congress include: the Notification of Risk to Personal Data Act, S. 239, 110th Cong. (2007); the Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); the Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); and the Cyber-Security Enhancement and Consumer Data Protection Act, H.R. 836, 110th Cong. (2007).

93. See S. 495, H.R. 958 (establishing requirements for data security); S. 239, H.R. 836 (establishing breach notification requirements).

94. See S. 239 § 9(f); S. 495 §§ 202(d), 303(d), 319(f); see also H.R. 958 § 4 (providing for enforcement only by administrative entities). But see H.R. 836 § 7(c), (e) (providing some immunity but otherwise leaving existing state laws in place).

95. S. 239 § 10; S. 495 §§ 203, 304; H.R. 958 § 6(a), (b). But see H.R. 958 § 6(c) (preserving state tort law).

96. See note 90, *supra*.

97. See text accompanying notes 32-35, *supra*.

specifically preempting states from protecting individuals' privacy rights in certain areas that could overlap the Act's coverage.<sup>98</sup>

Furthermore, proposed legislation seeks to eliminate states from being able to protect their citizens from breaches of the security of their personal information, a pervasive problem for privacy that leads to identity theft and is a consequence of modern database technology and information sharing.

The next section describes what privacy measures—properly enforced—can preserve, and why they are worthy of enforcement, enforcement that states should be able to provide where federal law does not.

*B. Privacy, Personhood, and Dignity—Why Privacy Matters*

Advances in technology that allow us to collect, disseminate, and analyze myriad personal events resemble, at least on the surface, the developments in photography and newspaper distribution that led Samuel Warren and Louis Brandeis to publish their 1890 *Harvard Law Review* article, "The Right to Privacy."<sup>99</sup> Warren and Brandeis were motivated by the need to protect individuals not from technology, but from the misuse of technology.<sup>100</sup> To them, the invasion of privacy involved a "spiritual" wrong, an injury to a man's "estimate of himself," and an assault upon "his own feelings."<sup>101</sup> They described the tort as protecting "peace of mind."<sup>102</sup> They proclaimed the principle of "inviolable personality" as giving rise to the right to privacy.<sup>103</sup> Warren and Brandeis were clear that meaningful remedies are part and parcel of this right.<sup>104</sup> Nonetheless, the modern privacy legislation described above provides remedies only spottily.<sup>105</sup>

To protect privacy is to recognize the Kantian principle of the innate dignity of persons.<sup>106</sup> To Immanuel Kant, dignity was an intrinsic

---

98. See text accompanying notes 44-48, *supra*.

99. 4 HARV. L. REV. 193 (1890). The authors, who deplored the "overstepping" of the press and the "numerous mechanical devices" that were breaching privacy, cited the "general right of the individual to be let alone" as the basis of the tort. *Id.* at 195-96, 205.

100. *Id.* at 195 (describing the impact of "[i]nstantaneous photographs" available to newspapers).

101. Warren & Brandeis, *supra* note 99, at 197.

102. *Id.* at 200.

103. *Id.* at 205.

104. See generally *id.*

105. See text accompanying notes 32 to 35, 59, and 80, *supra*.

106. See Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF MORALS 54 (Lewis White Beck trans., Bobbs-Merrill Co. 1969) (1785); see also Maxine D. Goodman, *Human Dignity in Supreme Court Constitutional Jurisprudence*, 84 NEB. L. REV. 740, 751 (2006).

quality, “a kind of value that all human beings have equally and essentially.”<sup>107</sup> Dignity and privacy both take notice of the personhood of each individual, and recognize that personhood as itself justifying recognition by others, a respect for the individual’s “inviolable personality,” freedom, and autonomy.<sup>108</sup> Dignity “can be said to refer to the status of individuals as ends in themselves, rather than as means toward some extraneous ends.”<sup>109</sup> By according individuals dignity we recognize that each is a “unique and irreplaceable human being.”<sup>110</sup> Zygmunt Bauman put it succinctly: “[d]ignity is the humanity of the humans.”<sup>111</sup>

If dignity recognizes the right of each individual to his or her own, unique “inviolable personality,”<sup>112</sup> privacy allows that personhood to develop.<sup>113</sup> In his concurring opinion in *Rosenblatt v. Baer*,<sup>114</sup> Justice Stewart emphasized the connections among dignity, personhood, and privacy: “the right of a man to the protection of his own reputation . . . reflects no more than our basic concept of the essential dignity and worth of every human being—a concept at the root of any decent system of ordered liberty.”<sup>115</sup>

The right to privacy as described by Warren and Brandeis “posit[s] the individual’s independence, dignity and integrity; it defines man’s

---

107. Hugo Adam Bedau, *The Eighth Amendment, Human Dignity, and the Death Penalty*, in *THE CONSTITUTION OF RIGHTS: HUMAN DIGNITY AND AMERICAN VALUES* 153 (Michael J. Meyer & William A. Parent eds., 1992).

108. Warren & Brandeis, *supra* note 99, at 205. See also Louis Henkin, *Human Dignity and Constitutional Rights*, in *THE CONSTITUTION OF RIGHTS: HUMAN DIGNITY AND AMERICAN VALUES*, *supra* note 107 (“[H]uman dignity requires respect for every individual’s physical and psychic integrity, for his ‘personhood’ before the law, [and] for her autonomy and freedom.”).

109. Herbert C. Kelman, *The Conditions, Criteria, and Dialectics of Human Dignity: a Transnational Perspective*, *INT’L STUDIES QUARTERLY* 21, 529, 531 (1977).

110. *Id.* at 532.

111. Zygmunt Bauman, *CHILDHOOD OF HUMAN DIGNITY, DIALOGUE AND UNIVERSALISM* 95 (2003).

112. Warren & Brandeis, *supra* note 99, at 205.

113. See Jonathan Kahn, *Privacy as a Legal Principle of Identity Maintenance*, 33 *SETON HALL L. REV.* 371, 378, 383 (2003). Professor Kahn observes that “[p]rivacy is valued insofar as it fosters the conditions within which an individual may establish, maintain and develop her identity as a core aspect of personhood. Thus conceived, invasions of privacy constitute an affront to human dignity by undermining one’s identity.” *Id.* at 382.

114. 383 U.S. 75 (1966).

115. *Id.* at 92 (Stewart, J., concurring). The Court explicitly linked dignity to liberty in *Lawrence v. Texas* by referring to the protection of liberty as preserving individuals’ “dignity as free persons.” 539 U.S. 558, 567 (2003). Along these same lines, Andrew Taslitz writes that “[t]o treat someone as a whole—as uniquely complete in himself—is status-enhancing, expressing the idea that each human is of equal and infinite worth.” Andrew E. Taslitz, *Respect and the Fourth Amendment*, 94 *J. CRIM. L. & CRIMINOLOGY* 15, 49 (2003).

essence as a unique and self-determining being.”<sup>116</sup> A breach of these standards inflicts, in the words of Edward Bloustein, “a blow to human dignity, an assault on human personality.”<sup>117</sup> To imperil privacy is to diminish dignity.

So how do each of the three federal laws, and the proposed federal personal information security legislation described above, relate to personhood, dignity, and privacy? The FCRA exists to ensure that third parties have a good reason to access information about individuals, and that such information is true and accurate.<sup>118</sup> Should that information be inaccurate, it would distort the person’s image and portray a false version of that person’s personality to the world at large.<sup>119</sup> Even when accurate, the disclosure of information outside of the permitted boundaries of the statute can harm dignity. Such a disclosure can impair the ability of a person to “control information about oneself and to have some limited dominion over the way one is viewed by society.”<sup>120</sup> The FCRA’s boundaries also curb the tendency of those in commerce to treat individuals, and their credit histories, as instruments to an end, a treatment that ignores individuals’ dignity.<sup>121</sup>

HIPAA shows an understanding that the business of our organs, cells, and genes is intensely personal and of great sensitivity. The revelation of such details to others may well leave one feeling every bit as exposed as when wearing an examining gown that gapes in the back. We may feel most vulnerable when ailing and in need of the help of health professionals. Vulnerability can also extend to our financial well-being. The risk that such information may be exposed raises anxiety over the impact it may have on others who may wield influence over that well-being. One may fear that insurers who acquire the information could decide that the information increases the risk of treatment too much, whether now or in the future. The fear raises the specter of unreimbursed medical bills piling high, threatening the security of those

---

116. Edward J. Bloustein, *Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964) (describing the authors’ motivation for their article as “a fear that a rampant press feeding on the stuff of private life would destroy individual dignity and integrity and emasculate individual freedom and independence”).

117. *Id.* at 974.

118. 15 U.S.C. § 1681b(a), (b) (2006) (describing permitted purposes for using a credit report).

119. See Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 550 (2006) (describing how distortion “involves the spreading of information that affects the way society views a person”). Professor Solove points out that though distortion hurts the person whose image is distorted, it “has effects for all of society . . . [w]e want to avoid arbitrary and undeserved disruption of social relations.” *Id.* at 551.

120. *Id.* at 550.

121. See Kant, *supra* note 106.

who depend on us. By requiring those in the medical industry to obtain consent under some circumstances before disclosing personal health information, HIPAA acknowledges that the items of medical information are not mere units in and of themselves, but connect to an integrated whole, a person who is worthy of respect and care.<sup>122</sup>

Similar to the FCRA, GLB recognizes that the information that financial institutions have can reveal many details, from credit card transactions to ATM use to account balances, and, when aggregated, can reveal more of our internal thoughts than any one single item of information could. In this age of information availability, the Act provides that financial institutions should honor the dignity of individuals by restraining themselves from freely releasing sensitive information until individuals have the opportunity to opt out of the institution's release of their data.

Finally, the proposed personal information security measures recognize the power of personal information, the risks of identity theft, and the damage that identity theft can do to others' perception of an individual. By requiring that those who hold such information take measures to protect it,<sup>123</sup> and acknowledging that individuals whose information is revealed to someone unauthorized to see it are entitled to learn of that disclosure,<sup>124</sup> these proposed personal information security provisions recognize the worth of one's "inviolate personality."<sup>125</sup>

However, each of these laws permits institutions to divulge a good deal of sensitive information. In contrast, meaningful privacy laws will protect "against the commercial exploitation of one's personality."<sup>126</sup> To the extent that the federal privacy laws discussed above facilitate trafficking in personal information by denying remedies, they risk demeaning the dignity of individuals whose information has been commodified, because doing so treats people as nothing more than the particular information traded.<sup>127</sup>

---

122. 45 C.F.R. § 164.502 (2008).

123. *See, e.g.*, H.R. 958 § 2.

124. *See, e.g.*, S. 239 § 2; H.R. 958 § 3.

125. Warren & Brandeis, *supra* note 99, at 205.

126. Hill v. Hayes, 240 N.Y.S.2d 286, 290 (N.Y. App. Div. 1963) (citing N.Y. Civ. RIGHTS Law § 51).

127. *See* Kelman, *supra* note 109, at 532. The trafficking in manifestations of personality injures personal dignity. *See* Bloustein, *supra* note 116, at 988 (describing the injury suffered when one's name or likeness is associated with a commercial product).

C. *Inadequate Agency Enforcement and the Impact of Rights without Remedies on Dignity and Privacy*

As discussed above, major federal privacy statutes by and large have a dearth of private enforcement available. Restrictions on or outright prohibition of private remedies and preemption of state laws create barriers to enforcement, which may encourage violations. However, conceivably vigorous public enforcement could make up for the loss of private enforcement. Each of the privacy statutes discussed above, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act, provide for enforcement by public officials.<sup>128</sup> Can such enforcement effectively vindicate, or at least advance, the privacy rights of individuals? As discussed below, whether aggressive administrative enforcement could stand in for the benefits of states' tort and statutory systems is an unanswered question, because the administrative agencies have been lax in enforcing the standards set by Congress. This laxity may well do damage not only to the dignity of individuals, but also to society as a whole.

1. *Problems of Administrative Enforcement*

Each of the three federal privacy statutes designates one or more federal agencies to enforce their provisions. For example, the Federal Trade Commission has primary enforcement power over the FCRA,<sup>129</sup> the Federal Trade Commission along with the federal banking agencies should enforce GLB,<sup>130</sup> and the Department of Health and Human Services should enforce HIPAA.<sup>131</sup> Given the amount of traffic in personal information, administrative agencies cannot provide blanket enforcement of the various acts' privacy protections. However, a substantial flaw in delegating significant (in the case of the FCRA) or sole (in the cases of HIPAA and GLB) responsibility for enforcement of these critical privacy rights to administrative agencies is that administrative agencies, whether for structural or political reasons, may allow the interests of those regulated by privacy statutes to outweigh the interests of the beneficiaries of these privacy statutes.

---

128. 15 U.S.C. §§ 6801s, 6805 (2006); 42 U.S.C. § 1320d-6 (2006).

129. 15 U.S.C. § 1681s(a). Other administrative agencies have FCRA enforcement power over institutions that they regulate. *Id.* § 1681s(b)(1).

130. *Id.* § 6805. These agencies include the National Credit Union Administration, the Department of the Treasury, the Securities and Exchange Commission, the Federal Reserve Board, and others. *Id.*

131. 42 U.S.C. § 1320d-5 (2006).

Regardless of the substance of any given statute, agency bias in favor of the regulated can undercut the effect of congressional allocations of rights and responsibilities, an allocation that gives substantial power to agencies when a statute restricts individuals' avenues for enforcement. Arguably, agencies owe special duties to the beneficiaries of statutory protections.<sup>132</sup> However, critics of agencies have asserted that agencies tend to favor the large, organized business entities regulated by federal statutes at the expense of less organized groups such as consumers and environmental interests.<sup>133</sup> Regulated interests may well have more access than individuals to agency decision makers, an imbalance of representation that may lead agencies to react favorably to the regulated.<sup>134</sup> Critics have asserted the "capture" theory, that "administrations are systematically controlled, sometimes corruptly, by the business firms within their orbit of responsibility."<sup>135</sup> Of course, less malignant factors may also influence agencies, such as the lack of institutional resources.

HIPAA, which allows no private enforcement, exemplifies the minimal impact of federal administrative enforcement on privacy interests. Although HIPAA relies on administrative enforcement, in that it does not allow private causes of action,<sup>136</sup> the Act's enforcer, the Department of Health and Human Services ("HHS"), has done very little to punish violators or obtain redress for individuals whose privacy has been lost. HHS has the power to impose \$100 for each violation, up to a maximum of \$25,000.<sup>137</sup> Under the George W. Bush administration, consumers filed nearly 20,000 privacy grievances under HIPAA through June 2006.<sup>138</sup> Nonetheless, HHS has prosecuted only four cases and

---

132. See Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1669, 1813 (1975). Stewart suggests that "[p]erhaps reviewing courts should give special weight to those interests that are likely to be 'underrepresented' in the informal agency process and hence have a lesser impact on the agency's policy decisions." *Id.* at 1787.

133. See *id.* at 1684-85.

134. *Id.* at 1713 (noting, among other benefits, that these groups can usually obtain a forum through which to force an agency to respond to the groups' view, and have the resources to "initiate" formal procedures).

135. *Id.* at 1685 (offering alternative explanations) (citations omitted).

136. See note 59, *supra*.

137. 42 U.S.C. § 1320d-6(b) (2006). Criminal violations could lead to penalties of up to \$250,000 in fines and 10 years in jail. *Id.*

138. Rob Stein, *Medical Privacy Law Nets No Fines*, WASH. POST, June 5, 2006, at A1 (noting that the agency under the Bush administration prosecuted only two criminal cases and imposed no fines whatsoever, notwithstanding the nearly 20,000 privacy grievances filed). Although the Office of Civil Rights seeks informal compliance whenever possible, 45 C.F.R. § 160.312 (2006), informal compliance has not provided restitution to individuals. See Kendra Gray, *The Privacy Rule: Are We Being Deceived?*, 11 DEPAUL J. HEALTH CARE L. 89, 103 (2008) (also noting that "OCR has investigated

imposed no fines whatsoever.<sup>139</sup> Rather, HHS prefers voluntary compliance.<sup>140</sup> A former head of the office that enforces HIPAA has said that staff size limited the office's ability to effectively resolve complaints.<sup>141</sup>

While this hands-off approach no doubt pleases those who are regulated, privacy advocates worry that such indulgence can lead industry participants to be sloppy when complying with the law.<sup>142</sup> An industry survey revealed that only 23% of those surveyed believed that their institutions were in full compliance with HIPAA's privacy requirements.<sup>143</sup> This indicates an expansive gulf between Congress's intent and the reality of self-regulation.

As for the FCRA, the Federal Trade Commission's catalog of its FCRA enforcement activities on its website reveals only a short list of actions since 2000.<sup>144</sup> Although one of those actions led ChoicePoint

---

only a fraction of the complaints it has received, and of those, it has resolved the complaint in favor of the health care provider or institution every time"); *see also* United States Department of Health and Human Services Office for Civil Rights, HIPAA Compliance and Enforcement, <http://www.hhs.gov/ocr/privacy/enforcement> (last visited June 23, 2008) (describing complaint investigation procedures).

139. Amy Lynn Sorrell, *Criminal HIPAA Case Targets Employee, Not Clinic, for Breach*, AMNews (July 14, 2008), available at <http://www.ama-assn.org/amednews/2008/07/14/gvsb0714.htm> (describing the fourth prosecution); Amy Lynn Sorrell, *3rd HIPAA Criminal Case Hints at Federal Tactics*, AMNews (Oct. 16, 2006), available at <http://www.ama-assn.org/amednews/2006/10/16/gvsb1016.htm>. *See also* Stein, *supra* note 138, at A1 (noting only two prosecutions up until that time).

140. Stein, *supra* note 138, at A1 (quoting Winston Wilkinson, then head of the Department of Health and Human Services' Office of Civil Rights, which is in charge of enforcing the law).

141. *Id.*

142. *Id.* (quoting one scholar as stating "I think we're dangerously close to having a law that is essentially meaningless").

143. AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION, THE STATE OF HIPAA PRIVACY AND SECURITY COMPLIANCE 3 (2005), [http://www.ahima.org/marketing/email\\_images/2005PrivacySecurity.pdf](http://www.ahima.org/marketing/email_images/2005PrivacySecurity.pdf). *See also* M.L. Baker, *HIPAA Compliance So-So and Stalling*, EWEEK.COM, Oct. 18, 2006, <http://www.eweek.com/c/a/Health-Care/HIPAA-Compliance-SoSo-and-Stalling/> (describing compliance with HIPAA's requirements as "lackluster" and stating that the number of health care providers fully complying with the Act was falling).

144. Federal Trade Commission Privacy Initiatives Enforcement, [www.ftc.gov/privacy/privacy/index.html](http://www.ftc.gov/privacy/privacy/index.html) (last visited June 23, 2008). Published agency actions on the site include the following: *In re* Milliman, Inc., No. 062-3189 (F.T.C. Feb. 6, 2008) (complaint and decision and order); *In re* Ingenix, Inc., No. 062-3190 (FTC Sept. 17, 2007) (complaint); *In re* Wright-Patt Credit Union, Inc., No. C-3171 (F.T.C. Apr. 12, 2003) (agreement containing consent order to cease and desist); *In re* Federated Department Stores, Inc., No. C-3175 (Apr. 1, 2003) (agreement containing consent order to cease and desist); *In re* Quicken Loans Inc., No. # 9304 (F.T.C. Dec. 30, 2002) (complaint); *Trans Union Corp. v. FTC*, No. 00-1141 (D.D.C. Feb. 13, 2001) (Final Order). *Id.* Other FTC actions include *U.S. v. ChoicePoint, Inc.*, No.1:06-CV-0198 (N.D. Ga. Jan. 30, 2006) (stipulated final judgment imposing \$10,000,000 in civil fines and \$5,000,000 in restitution); *U.S. v. Far West Credit, Inc.*, No. 2:06-CV-20041 (D.

Inc., to pay a fine of \$10,000,000 for violations of the FCRA and the FTC Act,<sup>145</sup> the agency has not followed up with similar fines against other FCRA violators. Studies of accuracy in credit reports, however, reveal widespread problems. A 2004 study found that 25 percent of the credit reports reviewed contained errors sufficiently serious to lead a creditor to deny credit.<sup>146</sup> Similarly, the Consumer Federation of America reported in 2002 that errors in consumer credit reports could cost consumers millions of dollars in higher costs for credit.<sup>147</sup> One consumer protection attorney testified before a congressional committee that he has pursued hundreds of FCRA actions on behalf of consumers successfully and that his office has more FCRA cases than can be handled,<sup>148</sup> indicating that substantially more violations occur than the FTC can pursue. The FTC might respond that it is not its role to vindicate every violation, but to choose those actions most likely to promote the public interest.<sup>149</sup> Nonetheless, where the FCRA denies

---

Utah Jan. 12, 2006) (consent decree); U.S. v. AT&T Corp., No. 022-3159 (N.D. N.J. Sept. 9, 2004) (consent decree); U.S. v. NCO Group, Inc., FTC File No., 922-3012 (C.D. Pa. May 12, 2004) (consent decree); U.S. v. Equifax Credit Info. Servs., No.1:00-CV-0087-MHS (N.D. Ga. July 29, 2003) (joint motion for modification of consent decree); FTC v. Citigroup, Inc., C.A., No. 010CV-0606 (N.D. Ga. Sept. 18, 2002) (stipulation of settlement); U.S. v. Performance Capital Mgmt., Inc., No. 9823542 (C.D. Cal. Aug. 24, 2000) (consent decree); U.S. v. Trans Union LLC, No. 00C 0235 (N.D. Ill. Jan. 12, 2000) (consent decree); U.S. v. DC Credit Servs., Inc., No. 02-5115 (D.C. Cal. June 27, 2002) (consent decree); U.S. v. Equifax Credit Info. Servs., Inc., No. 1:00-CV-0087 (N.D. Ga. Jan. 12, 2000) (consent decree).

145. See *United States v. ChoicePoint Inc.*, No. 1-06-CV-0198 (N.D. Ga. Jan. 30, 2006), available at <http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf> (stipulated final judgment).

146. ALISON CASSIDY & EDMUND MIERZWINSKI, MASSPIRG EDUCATION FUND, MISTAKES DO HAPPEN: A LOOK AT ERRORS IN CONSUMER CREDIT REPORTS 6, 11 (2004), <http://static.masspirg.org/reports/MistakesDoHappen2004MA.pdf> [hereinafter MISTAKES]. The study by the Massachusetts Public Interest Research Group in 2004 of 154 consumers and their credit reports found that 79% of the credit reports contained mistakes; one in four contained serious errors that could result in the denial of credit; nearly one in three contained credit accounts listed as open that had been closed by the consumer. *Id.* at 4.

147. CONSUMER FEDERATION OF AMERICA AND NATIONAL CREDIT REPORTING ASSOCIATION, CREDIT SCORE ACCURACY AND IMPLICATIONS FOR CONSUMERS 35 (2002), [http://www.consumerfed.org/121702CFA\\_NCRA\\_Credit\\_Score\\_Report\\_Final.pdf](http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf). In 2003, the U.S. General Accounting Office concluded that more study concerning the accuracy of credit reports is needed. See generally U.S. GEN. ACCOUNTING OFFICE, CONSUMER CREDIT: LIMITED INFORMATION EXISTS ON THE EXTENT OF CREDIT REPORT ERRORS AND THEIR IMPLICATIONS FOR CONSUMERS (2003).

148. LEONARD A. BENNETT, WRITTEN TESTIMONY BEFORE THE H. COMM. ON FINANCIAL SERVICES, REGARDING "FAIR CREDIT REPORTING ACT: HOW IT FUNCTIONS FOR CONSUMERS AND THE ECONOMY" 2 (2007), available at <http://www.naca.net/assets/shared/633201869867878750.pdf>. These actions would have been based on those provisions for which the FCRA permits a private cause of action.

149. See 16 C.F.R. § 2.3 (2008) (stating, with respect to nonadjudicative procedures, that "[t]he Commission acts only in the public interest and does not initiate an

private remedies and preempts state protections, violators can largely be comfortable that they are free from sanctions, leaving individuals' privacy to their mercy.

Furthermore, Congress significantly constrained the power of the FTC to pursue certain violations of the FCRA by furnishers. The FTC may not impose a civil penalty on a furnisher for violating its duty to provide only accurate information to consumer reporting agencies<sup>150</sup> unless the furnisher has been previously enjoined from committing the violation, or ordered not to commit it, and the furnisher has subsequently violated the injunction or order.<sup>151</sup> Given that furnishers are free from concerns of liability to individuals for violating this standard,<sup>152</sup> the leash on administrative enforcement leaves them relatively free from concern of incurring costs for violating this aspect of the FCRA.

None of the agencies charged with enforcing GLB's privacy provisions took any enforcement action with respect to the Financial Privacy Rule in the first two years of the Act.<sup>153</sup> The FTC took enforcement actions against a handful of financial service providers for violating the Act's privacy provisions over a five year span.<sup>154</sup> Between

---

investigation or take other action when the alleged violation of law is merely a matter of private controversy and does not tend adversely to affect the public").

150. 15 U.S.C. § 1681s-2(a)(1) (2006).

151. *Id.* § 1681s(a)(3). Furthermore, a court may not impose any civil penalty for any violation of the Act occurring before the violation of the injunction or order. *Id.*

152. *See id.* § 1681s-2(c).

153. U.S. GEN. ACCOUNTING OFFICE, REPORT TO CONGRESSIONAL COMMITTEES, FINANCIAL PRIVACY: TOO SOON TO ASSESS THE PRIVACY PROVISIONS IN THE GRAMM-LEACH-BLILEY ACT OF 1999, 7 (2000), [www.gao.gov/new/items/d01617.pdf](http://www.gao.gov/new/items/d01617.pdf). The FTC did successfully defend a claim by a trade association representing consumer reporting agencies and their customers that sought to overturn GLB's regulations. *See generally* Individual Reference Serv. Group v. FTC, 145 F. Supp. 2d 6 (D.D.C. 2001), *aff'd sub nom.* Trans Union v. FTC, No. 01-5202 (D.C. Cir. 2002).

154. *See* U.S. GEN. ACCOUNTING OFFICE, REPORT TO S. COMM. ON BANKING, HOUSING & URBAN AFFAIRS, PERSONAL INFORMATION: KEY FEDERAL PRIVACY LAWS DO NOT REQUIRE INFORMATION RESELLERS TO SAFEGUARD ALL SENSITIVE DATA 50-51, n.89, (2006) [hereinafter GAO Report on Privacy Laws]. The actions taken by the FTC include *In re Nations Title Agency, Inc.*, No. C-4161, 2006 WL 1967073 (F.T.C. June 19, 2006) (complaint); *In re Nationwide Mortg. Group, Inc.*, No. 9319, 2005 WL 996696 (F.T.C. Apr. 12, 2005) (complaint alleging violations of both the Financial Privacy Rule and the Safeguards Rule); *In re Sunbelt Lending Servs., Inc.*, No. C-4129, 2005 WL 120875 (F.T.C. Jan. 3, 2005) (complaint alleging violations of both the Financial Privacy Rule and the Safeguards Rule); *In re Sunbelt Lending Servs., Inc.*, No. 042-3153, 2004 WL 2682802 (F.T.C. Nov. 16, 2004) (complaint alleging violations of both the Financial Privacy Rule and the Safeguards Rule); *In re Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004) (complaint). *See also*, FTC v. Debt Mgmt. Found. Serv., Civ. No. 8:04-CV-EAK-MSS (M.D. Fla. Mar. 29, 2005).

As the cases above indicate, the FTC has put some energy into enforcing GLB's Safeguards Rule, 16 C.F.R. pt. 314. *See, e.g.*, *In re Nations Title Agency, Inc.*, No. 052-3117 (F.T.C. June 19, 2006) (decision and order); *In re Superior Mortg. Corp.*, No. C-4153, 2005 WL 3524927 (F.T.C. Dec. 14, 2005) (complaint); *In re Nat'l Research Ctr.*

2002 and 2005, the FDIC took only twelve formal enforcement actions for violations of GLB,<sup>155</sup> and no formal FCRA actions.<sup>156</sup>

Paltry agency enforcement of these federal privacy laws has a magnified impact on privacy where tort law cannot step in to fulfill its traditional role. As discussed below, tort law serves to deter persons from acting in a way that violates social norms and undermines human flourishing. Accordingly, to immunize actors from liability for illegal conduct can remove that deterrent effect, causing them to act in such a way as to inflict harmful behavior on others. The impact of that removal swells when not only tort claims, but also statutory enforcement and administrative oversight vanish. From a law and economics perspective, “legal rules should force actors to take account of the costs of their activities.”<sup>157</sup> With minimal enforcement, public or private, these federal privacy laws become, at most, “a hope or a wish.”<sup>158</sup>

## 2. *The Impact of Remediless Federal Privacy Rights.*

Having a limited right to a private cause of action (in the case of the FCRA) and no right at all (in the case of GLB and HIPAA), these federal privacy laws may well fail to exact compliance with the standards they purport to impose. This failure can hurt not just individuals, but society as well.

First, the violation of these standards hurts individuals’ privacy, and, thereby, their dignity. As an example with respect to the FCRA, an individual may deal with a merchant that falsely reports that the person reneged on a bill, perhaps due to a clerical error in the merchant’s books. Making such a false report may well violate the Act’s requirement that

---

for Coll. & Univ. Admissions, No. 022-3005 (F.T.C. Oct. 2, 2002); *FTC v. XTEL Mktg., Inc.*, No. 04C7238e (N.D. Ill. Nov. 9, 2004) (complaint).

The FTC has also taken action to enforce its rule regarding the safe disposal of consumer credit report information, 16 C.F.R. pt. 682. See *FTC News, Company Will Pay \$50,000 Penalty*, <http://www.ftc.gov/opa/2007/12/aumort.shtm> (news release publicizing stipulated judgment and order ordering payment of \$50,000 fine).

155. GAO Report on Privacy Laws, *supra* note 153, at 43. Since then the FDIC has taken a few more actions, but to enforce the Safeguards Rule rather than the Financial Privacy Rule. See generally *In re USA Bank*, No. 07-2-6b (Oct. 22, 2007) (order to cease and desist pertaining to information security); *In re SouthwestUSA Bank*, No. 06-216b (Nov. 9, 2006) (order to cease and desist); *In re Columbia Savings Bank*, No. 07-183b (Nov. 13, 2007).

156. See GAO Report on Privacy Laws, *supra* note 153, at 43. The Office of the Comptroller of the Currency took 18 actions between October of 2000, and September of 2005. *Id.* The Federal Reserve Bank, which also has FCRA enforcement authority, took none in the first five years of this decade. *Id.*

157. Thomas C. Galligan, Jr., *Deterrence: The Legitimate Function of the Public Tort*, 58 WASH. & LEE L. REV. 1019, 1032 (2001).

158. Donald H. Ziegler, *Rights Require Remedies: A New Approach to the Enforcement of Rights in the Federal Courts*, 38 HASTINGS L.J. 665, 678 (1987).

the furnisher take care to provide accurate information.<sup>159</sup> The false item could cripple the individual's ability to obtain credit, or even to maintain the current credit terms in place.<sup>160</sup> Nonetheless, the injured individual may have no real recourse. The FCRA, while prohibiting such false reporting, expressly denies individuals the right to sue over it.<sup>161</sup> The Federal Trade Commission could, but likely would not, seek to force the furnisher to comply with its responsibilities.<sup>162</sup> State authorities could also bring an action, but are restrained by the Act's advance notice requirements that limit such authorities' ability to recover damages for initial violations of some of the most important restrictions.<sup>163</sup> These authorities also suffer the same constraints on resources that federal agencies face.<sup>164</sup> By limiting enforcement to administrative agencies, budget and personnel constraints can starve these rights into obscurity.

So, with no right to enforce the statutory "right," the injured individual could bring a defamation action under state law. However, the FCRA anticipates that action and prohibits such use of state law unless the injured individual can show that the furnisher acted with actual malice or willful intent to injure.<sup>165</sup> Other state remedies would likely be foreclosed by the Act's preemption provisions.<sup>166</sup> The injury to reputation, to privacy, and to dignity will go untreated, and the offender can remain free from compensation concerns that could encourage it to modify its business practices to mind the dignity of the individual lives it touches.<sup>167</sup>

The consequences of a failure to enforce HIPAA are similar. Here, the federal statute has not preempted state remedies, at least those that are not less favorable than HIPAA's privacy provision.<sup>168</sup> However,

---

159. See 15 U.S.C. § 1681s-2(a) (2006).

160. See generally Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 VAL. U. L. REV. 1061 (2007) (describing the kinds of impacts that negative information in a credit report can have on a consumer).

161. 15 U.S.C. § 1681s-2(c).

162. *Id.* § 1681s. The FTC would be unlikely to pursue a case that impacted only one individual.

163. *Id.* § 1681s(c)(5).

164. See *infra* text accompanying notes 171, 210-16.

165. 15 U.S.C. § 1681h(e). The immunity would arise if the disclosure arose from one of the provisions specified. *Id.*

166. See *id.* § 1681t(b)(1)(F). The preemption provision preserves two preexisting state statutes, one from California and one from Massachusetts. *Id.* § 1681t(b)(1)(F)(1), (ii).

167. The individual could pursue correction of the item through the Act's requirement that agencies, once notified of an inaccurate item, must try to verify it with the item's furnisher. See *id.* § 1681i.

168. Pub. L. 104-191, § 264(c)(1), 110 Stat. 1936 (1996) (codified at 42 U.S.C. § 1320d-2 (2000)).

HIPAA's main flaw is that its denial of a private cause of action stretches much more broadly than does the FCRA's selective denial, which leaves some rights open for private enforcement.<sup>169</sup> HIPAA creates some rights to maintain the privacy of medical information, but fails to back them up with any meaningful recourse for redress. The danger of this practice is that regulated entities—hospitals, doctors, and other participants in the medical industry—may be aware of the standards and yet be complacent about complying with them, given the lack of rigor that the Department of Health and Human Services' Office of Civil Rights has shown in enforcing the Act's privacy provisions.<sup>170</sup> At the same time, however, the publicizing of the privacy rights may give individuals a false sense of security, causing them to drop their guard and disclose sensitive information they may have kept private had they realized the Act's absence of teeth. Accordingly, individuals may end up losing privacy instead of gaining it.

Similarly, news of the privacy provisions of GLB does not usually carry with it the warning that they are rights in name only.<sup>171</sup> To the extent people even understand that they have the ability to opt out of the sharing of their private financial information,<sup>172</sup> they may not understand that institutions may well suffer no consequences whatsoever for violating GLB's restrictions on information disclosure.

The lack of private enforceability of the standards set by federal personal privacy statutes may have loosened privacy protection, notwithstanding Congress's pronouncement of specific standards of behavior. For example, evidence indicates that even GLB's weak privacy protections, intended in part to curb profligate sharing of personal information among financial institutions, are widely ignored.<sup>173</sup> The Act does not provide individuals the tools with which to learn whether institutions are revealing private information, and so individuals have a difficult time learning whether the Act has been violated and by whom. Widespread sharing of personal information without notice may occur, invisible to the individual whose information is on display. So

---

169. See, e.g., 15 U.S.C. §§ 1681b, 1681e, 1681i; see also *id.* §§ 1681n, 1681o (the private cause of action provisions of the FCRA).

170. See text accompanying notes 136 to 143, *supra*.

171. See, e.g., Don Oldenburg, *Protecting Your Financial Privacy*, WASH. POST, July 27, 2001, at C12.

172. See 15 U.S.C. § 6802(b)(1); 16 C.F.R. § 313.10(a)(1) (2008). Privacy notices issued under GLB have been criticized for their readability. Mark Hochhauser, *Lost in the Fine Print: Readability of Financial Privacy Act Notices* (July, 2001), available at <http://www.privacyrights.org/ar/GLB-Reading.htm>.

173. See James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 43 (2005).

long as the regulatory agencies do not police day-to-day compliance, that compliance becomes, as James Nehf has written, “largely voluntary.”<sup>174</sup>

Actions that corporations may take without much fear of consequences include the disclosure of account information to third parties, information that might reveal what an individual buys, when, and for how much. If companies do not abide by their obligation to notify consumers of institutional privacy policies,<sup>175</sup> an individual may never learn that his or her personal information can be widely disseminated. Although federal law guarantees to individuals the right to opt out of many disclosures of personal information, if a company violates the statutory obligation to allow each individual an opportunity to opt out, that individual is powerless to restrain the institution’s disclosure, sale, or other use of the information.<sup>176</sup> By providing a standard and then failing to enforce it, federal law comes close to inviting the very behavior that it appears to prohibit.

Without private remedies, the federal acts lose all the benefits of the private attorney general, the deterrence and standard-defining effects that arise from litigation brought by those who are harmed by the violations. In the case of privacy, that means that we are losing an opportunity to help further define the types of behaviors that breach the norms Congress intended to govern.

Given the evidence thus far, we can anticipate the effects of a federal personal information security law, as described above, if that law has no private enforcement remedies and preempts the many state laws that have arisen that require those with sensitive data to notify individuals when they have lost control of that data.<sup>177</sup> Were certain bills to pass that are currently pending in Congress, no one whose data was treated carelessly, in a way that would violate both a state law and the proposed federal law, would have any ability to enforce it.<sup>178</sup> Rather, only federal agencies and state attorneys general would have the power to enforce the standards.<sup>179</sup> Since administrative enforcement of other federal privacy statutes has been so loose, we could anticipate that very few actions, if any, would be brought against those who flouted the new law, no matter how egregious the infractions. Those injured by the breach would naturally turn to state personal information security laws,

---

174. *Id.* at 1.

175. *See* 15 U.S.C. § 6803(a).

176. *See id.* § 6802(b)(1); 16 C.F.R. § 313.1(a)(1).

177. *See* statutes cited at note 90, *supra*.

178. *See* S. 239, 110th Cong. § 10 (Jan. 10, 2007); S. 495, 110th Cong. §§ 202(d), 303(d), 319(f) (Feb. 6, 2007); H.R. 958, 110th Cong. §§ 4, 6 (Feb. 8, 2007). *But see* H.R. 836, 110th Cong. §§ 7(c), (e) (providing some immunity but otherwise leaving existing state laws in place).

179. *See* S. 239 §§ 8, 9; S. 495 §§ 202, 203, 303, 304, 317, 318, 303(d).

only to find that Congress has struck them down with its power to preempt. Nonetheless, publicity surrounding such a federal law would likely not highlight the lack of power to enforce it and, thus, individuals might well be deceived into thinking that congressional action had actually enhanced, rather than reduced, the security of personal information held by institutions. Such false security might well lead individuals to take *less* rather than *more* care with their personal information.

Altogether, these federal privacy rights portray an image of national protection, of restraining the technological advances that can reveal so much so quickly. Yet, without remedies and without meaningful enforcement, the standards run the danger of becoming mere suggestions. Regulated institutions may perceive no recognizable downside to breaching these standards, where revealing credit histories, financial transaction information, and details of health records may all be traded and sold.

The loss is not for individuals alone, but for individuals collectively, that is, for society. We may become deceived, being careless with our information because we believe that *de jure* limitations will be *de facto* limitations. This false sense that legal standards are observed may lead individuals to treat their personal information with less care, or with less discretion. We may think of the privacy laws as a group that collectively shields us, but we do not realize the barrier is illusory.

## II. THE TRADITION OF RIGHTS AND REMEDIES—FEDERALISM AND ENFORCEMENT

### A. *The Tradition of State Torts*

The federalization of privacy rights veers from a long tradition that vests the responsibility for citizens' well-being in the states and their torts. The tort system exists to force wrongdoers to account for "damages inflicted or injuries caused, whether by malfeasance, misfeasance, or nonfeasance."<sup>180</sup> Though civil tort actions developed from criminal actions, and became distinct from those actions, torts continued to provide a punitive function to address those who breach acceptable social norms.<sup>181</sup> That these norms develop in the hearth of the local community is reflected in the legal standards that we still use;

---

180. Michael L. Rustad, *Smoke Signals from Private Attorneys General in Mega Social Policy Cases*, 51 DEPAUL L. REV. 511, 527 (2001).

181. *Id.* at 519-20.

negligence, for example, is judged in the eye of a normal member of the community.<sup>182</sup>

States make moral choices through their development of tort law, selecting “the essential needs and requirements of mankind.”<sup>183</sup> Through torts, the justice system encourages a culture of care,<sup>184</sup> one that fosters the capacity for individuals to develop a tailored version of the Aristotelian “good life.”<sup>185</sup> Thus, tort law deters conduct that the state has determined undermines human flourishing.<sup>186</sup>

The Supreme Court has emphasized that states have “a significant interest in redressing injuries that actually occur within the State.”<sup>187</sup> The Court has acknowledged the special role of state common law torts and the interests of the state in protecting its citizens by upholding the rights of such citizens to employ state common law torts even where Congress has usurped the underlying area for regulation. For example, in *Silkwood v. Kerr-McGee Corp.*,<sup>188</sup> the administrator of the estate of a laboratory analyst, who had worked at a federally-licensed nuclear facility, brought suit pursuant to Oklahoma common law after the analyst became contaminated from plutonium at the facility.<sup>189</sup> The defendant argued

---

182. Oliver Wendell Holmes, *Lecture IV: Fraud, Malice, and Intent—The Theory of Torts*, in *THE COMMON LAW* 130, 162 (1881) (arguing that the standard should be “whether his conduct would have been wrong in the fair average member of the community, whom he is expected to equal at his peril”).

183. Thomas Poole, *Back to the Future? Unearthing the Theory of Common Law Constitutionalism*, 23 *OXFORD J. LEGAL STUD.* 435, 440 (2003) (discussing the role of the common law and constitutions in promoting the public good).

184. Nelson P. Miller, *Seven Conceptual and Historical Errors in Tort Law*, 40 *TORT TRIAL & INS. PRAC. L.J.* 59, 68 (2004) (“[T]ort law is a guidepost to a better life—for both the careless actor and the potential recipient of the careless action.”).

185. See generally MARTHA NUSSBAUM, *THE FRAGILITY OF GOODNESS: LUCK AND ETHICS IN GREEK TRAGEDY AND PHILOSOPHY* (Cambridge rev’d ed. 2001) chs. 8-12; see also LON FULLER, *THE MORALITY OF LAW* 5 (1969) (“The morality of aspiration is most plainly exemplified in Greek Philosophy[;] [i]t is the Good Life, of excellence, of the fullest realization of human powers.”).

186. See, e.g., Thomas C. Galligan, Jr., *Deterrence: The Legitimate Function of the Public Tort*, 58 *WASH. & LEE L. REV.* 1019, 1031 (2001); Jeffrey J. Rachlinski, *Misunderstanding Ability, Misallocating Responsibility*, 68 *BROOK. L. REV.* 1055, 1058 (2003); see also *Friends for All Children, Inc. v. Lockheed Aircraft Corp.*, 746 F.2d 816, 825 (D.C. Cir. 1984) (noting that the two principal purposes of tort law are “the deterrence of misconduct and the provision of just compensation to victims of wrongdoing”); *Cenco Inc. v. Seidman & Seidman*, 686 F.2d 449, 455 (7th Cir. 1982) (describing the “underlying objectives of tort liability [to be] to compensate the victims of wrongdoing and to deter future wrongdoing”); *Thompson v. Sun City Cmty. Hosp., Inc.*, 688 P.2d 605, 615 (Ariz. 1984) (noting that “deterrence of negligent conduct” is “one of the primary functions of the tort system”); *RESTATEMENT (SECOND) OF TORTS* § 901(c) (1979) (citing deterrence of wrongful conduct as one purpose of tort actions).

187. *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 776 (1984).

188. 464 U.S. 238 (1984).

189. *Id.* at 242-43.

that the Price-Anderson Act, a federal act that regulated the safety of the nuclear energy industry, overrode any right of the plaintiff to seek remedies from state common law.<sup>190</sup> However, the Court rejected that argument, upholding the plaintiff's right to seek the punitive damages that state law authorized.

In addition to deterring harmful conduct that impedes human flourishing, state tort law can adapt and evolve because it has an organic quality that responds to its environment. State tort law also has the ability to attend to the particular details of a given situation, and in that way to acknowledge the complexity of human life and human interactions.<sup>191</sup> Tort law allows states to develop diverse policies that suit the needs of their particular citizens by recognizing and honoring states' interests in allowing their citizens to enforce local norms.<sup>192</sup> In addition, it allows states to flexibly accommodate the shifting needs of their citizens by adapting old torts or even by creating new ones.<sup>193</sup> The common law, by changing shape with each new decision, can "embody the fundamental values of a society" as those values shift over time and respond to developments in technology, industry, and moral reasoning.<sup>194</sup> It has a record of adapting over centuries to societies' needs as they evolve: "It is the peculiar merit of the common law that its principles are so flexible and expansive as to comprehend any new wrong that may be developed by the inexhaustible resources of human depravity."<sup>195</sup> An

---

190. *Id.* at 256. "It may be that the award of damages based on the state law of negligence or strict liability is regulatory in the sense that a nuclear plant will be threatened with damages liability if it does not conform to state standards, but that regulatory consequence was something that Congress was quite willing to accept." *Id.* In contrast, where the regulated area is "'a field which the States have traditionally occupied,'" a federal regulation may be much more likely to preempt a state tort action. *Buckman Co. v. Plaintiffs' Legal Comm.*, 531 U.S. 341, 347 (2001) (quoting *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947)).

191. See THOMAS ATKINS STREET, *THE FOUNDATIONS OF LEGAL LIABILITY: A PRESENTATION OF THE THEORY AND DEVELOPMENT OF THE COMMON LAW* xxiii (1906).

192. For example, states have developed different standards of care regarding the liability for escaped water. See Betsy J. Grey, *The New Federalism Jurisprudence and National Tort Reform*, 59 WASH. & LEE L. REV. 475, 514 (2002) (describing such choices as being based on the particular economic needs of each state). The article describes a number of other areas in which states have developed different standards. *Id.* at n.209.

193. *Id.* at 514-15.

194. See Poole, *supra* note 183, at 445 (quoting T.R.S. ALLAN, *CONSTITUTIONAL JUSTICE: A LIBERAL THEORY OF THE RULE OF LAW* 19 (Oxford: Clarendon Press, 2001)).

195. *Johnson v. Girdwood*, 58 N.Y. St. Rep. 338 (1894). Thomas Atkins Street lauded the "complexity" of the common law as reflecting the complexity of human life and human intercourse. "The common law is really the very embodiment of the spirit of law. The dominance of this spirit is conspicuously shown in its wonderful tenderness for facts and its singular patience in working out details. A genius for searching out external truth is the peculiar mark and the peculiar strength of the English common law." STREET, *supra* note 191, at xxiii.

early torts scholar described the common law as “an organism which is almost purely of natural growth.”<sup>196</sup>

Not only does tort law allow states to adapt to the needs of society and its citizens by adapting the use of old traditional torts, but it also can expand with new torts to respond to those needs. Justice Brandeis observed that “[i]t is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”<sup>197</sup>

Privacy torts, which were gradually adopted after Warren and Brandeis’s groundbreaking article,<sup>198</sup> exemplify just that sort of response. Invasion of privacy actually comprises four different torts: appropriation, false light in the public eye, unreasonable intrusion, and public disclosure of private facts.<sup>199</sup> These torts are described in more detail below. Torts that can protect values similar to those advanced by the privacy torts include defamation, breach of confidentiality, and intentional infliction of emotional distress.<sup>200</sup> The flexibility of tort law is revealed by the ways states have picked and chosen among these available actions. Nearly every state recognizes at least one form of the tort, some through statute rather than by common law;<sup>201</sup> however, states may recognize one without recognizing another. For example, Minnesota has declined to recognize the false light tort, while adopting the other three privacy torts.<sup>202</sup> New York has chosen not to treat privacy as a common law tort subject, and instead addressed the injury through state statute.<sup>203</sup>

Recent evidence of this plasticity of tort law is found in the developing field of cyberspace law. Michael Rustad and Thomas Koenig, privacy scholars, have emphasized the importance of torts in

---

196. STREET, *supra* note 191, at xxiii. Street later noted that “[a] fact which is to-day recognized as parasitic will, forsooth, to-morrow be recognized as an independent basis of liability. It is merely a question of social, economic, and industrial needs as those needs are reflected in the organic law.” *Id.* at 470.

197. *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (Brandeis, J., dissenting). *See also* *Gregory v. Ashcroft*, 501 U.S. 452, 458 (1991); *Garcia v. San Antonio Metro. Transit Auth.*, 469 U.S. 528, 567 n.13 (1985) (all noting the value of the federalist structure); *FERC v. Mississippi*, 456 U.S. 742, 787-88 (1982) (O’Connor, J., dissenting in part).

198. *See* Warren & Brandeis, *supra* note 99.

199. *See generally* Keeton, *supra* note 76, at 849-69; RESTATEMENT (SECOND) OF TORTS §§ 652B-652E (1979).

200. *See* *Alexander v. Culp*, 705 N.E.2d 378 (Ohio Ct. App. 1997) (recognizing the duty of a member of the clergy to keep parishioner’s information confidential); *Doe v. Roe*, 400 N.Y.S.2d 668 (N.Y. App. Div. 1977) (recognizing a similar duty for a psychoanalyst to a patient); RESTATEMENT (SECOND) OF TORTS §§ 46, 558.

201. *See, e.g.*, N.Y. CIV. RIGHTS LAW § 50 (McKinney 2008).

202. *See* *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998).

203. *See* N.Y. CIV. RIGHTS LAW § 50 (McKinney 2008).

balancing the interests of industry participants and individuals: “Tort rights and remedies must be strengthened so that they can play their traditional social control role in the information age; an era in which the nature of injuries has been transformed from tangible, physical harms to intangible injuries to privacy, reputation and individual dignity.”<sup>204</sup> Tort law’s ability to adapt to changing technology and norms gives it a powerful advantage over the federal privacy enactments discussed above.

In sum, through a system of torts, localities can promote the individuality of their citizens and foster the inquiry for the “good life,” can adapt to changes in the social norms that govern individuals’ relations with one another, and can create new torts that reflect changes in personal development, in technology, and in society. Discussed below are some of the features of state privacy laws.

## B. State Privacy Protection

### 1. State Privacy Protection through Common Law Torts

Invasion of privacy comprises a quartet of torts developed at common law that protect individuals from privacy breaches and information disclosures. Appropriation involves the use, for the defendant’s benefit, of the plaintiff’s name or likeness.<sup>205</sup> False light in the public eye allows an action for publicity that places a person in a false light where that publicity is highly offensive to the ordinary person, even if the publicity is not defamatory.<sup>206</sup> Unreasonable intrusion into seclusion allows a cause of action for the intentional interference with a person, or that person’s private affairs.<sup>207</sup> Public disclosure of private

---

204. Michael L. Rustad & Thomas Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOK. L. REV. 1, 6 (2002). The authors go on to trace tort history, arguing that through the Industrial Revolution tort immunities granted to negligent actors, such as contributory negligence and the English fellow servant rule, bred “corporate irresponsibility.” *Id.* at 28-29.

205. See Keeton, *supra* note 76, at 851; RESTATEMENT (SECOND) OF TORTS § 652C (1979); see also Sloan v. S.C. Dept. of Pub. Safety, 586 S.E.2d 108, 110 (S.C. 2003) (because state law authorized sale of images on drivers’ licenses, no liability for misappropriation).

206. RESTATEMENT (SECOND) OF TORTS § 652E. The First Amendment strictly limits awards under this tort when the information concerns public figures or matters of public interest. See, e.g., *Time, Inc. v. Hill*, 385 U.S. 374 (1967) (applying *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), to hold no recovery for false light for publication of fictionalized version of plaintiffs’ hostage experience, portrayed as re-enactment, without showing actual malice).

207. Keeton, *supra* note 76, at 854; RESTATEMENT (SECOND) OF TORTS § 652B.

facts prohibits the disclosure of private facts to the public when such disclosure would be highly offensive to a reasonable person.<sup>208</sup>

These torts in their original forms protect privacy imperfectly. For example, the tort of public disclosure of private facts, as construed before the advent of widespread use of technology, required proof that publicity was given to matters concerning the plaintiff's private life, that publication of those matters would be highly offensive to a reasonable person of ordinary sensibilities, and that the matter publicized was not of legitimate public concern.<sup>209</sup> The publicity element can be difficult to satisfy for those who have suffered from a humiliating disclosure to only one or a few. Nevertheless, the adaptability of the common law appears in the decision of a court in Wisconsin, which adjusted this element in just the sort of manner typical of the evolution of common law torts. The Wisconsin court upheld an invasion of privacy verdict based on a single disclosure to a single person, stating that the jury may consider the type and character of the person to whom the defendant disclosed the information in determining whether the plaintiff satisfied the publicity element of the tort.<sup>210</sup> In a similar example of growth, some courts have ruled that if the persons to whom the defendant discloses the private matter have a special relationship with the plaintiff, disclosure to just a couple of people may satisfy the disclosure element.<sup>211</sup> These examples of adaptation offer models for courts that face claims involving changes

---

208. Keeton, *supra* note 76, at 856-57; RESTATEMENT (SECOND) OF TORTS § 652D.

209. See, e.g., Phillips v. Grendahl, 312 F.3d 357, 371-72 (8th Cir. 2002); Johnson v. Sawyer, 980 F.2d 1490 (5th Cir. 1992) (applying Texas law), *rev'd*, 47 F.3d 716 (5th Cir. 1995) (en banc), *vacated and remanded after remand*, 120 F.3d 716 (5th Cir. 1997); Robins v. Conesco Fin. Loan Co., 656 N.W.2d 241 (Minn. Ct. App. 2003).

210. Pachowitz v. Ledoux, 666 N.W.2d 88 (Wis. Ct. App. 2003). Similarly, a federal appeals court upheld a jury's verdict that a single disclosure of a love letter and a wife's diary to the wife's husband could yield liability for public disclosure of private facts under Kentucky law. *McSurely v. McClellan*, 753 F.2d 88, 113 (D.C. Cir. 1985).

211. See *Chisholm v. Foothill Capital Corp.*, 3 F. Supp. 2d 925, 941 (N.D. Ill. 1998) (disclosure of plaintiff's affair with a married man to two of her potential business clients could satisfy publicity element; however, plaintiff failed to show that the information was private and that its disclosure would be highly offensive to a reasonable person, therefore action dismissed). See also *Hill v. MCI WorldCom Comm'ns, Inc.*, 141 F. Supp. 2d 1205, 1212-13 (S.D. Iowa 2001) (telecommunications carrier's disclosure to customer's ex-husband of customer's billing information and names of parties she'd called stated claim because of special relationship between customer and ex-husband); *Munoz v. Chicago School Reform Bd. of Bd. of Trustees*, No. 99 C 4723, 2000 WL 152138, at \*10 (N.D. Ill. Feb. 4, 2000) (teacher who alleged that her personnel file was disclosed to students' parents met publicity element because she had a special relationship with those parents); *Pinkston-Adams v. Nike, Inc.*, No. 99 C 1044, 1999 WL 543202, at \*4 (N.D. Ill. July 22, 1999) (communication of personal information to plaintiff's employees could meet publicity element); *Miller v. Motorola, Inc.*, 560 N.E.2d 900, 903 (Ill. Ct. App. 1990) (plaintiff could meet publicity element of tort based on employer's disclosure of her surgery to her co-workers because of her special relationship with them).

in information technology, such as that allowing mass aggregation and analysis of disparate bits of data. Such a court could similarly reinterpret a privacy tort element in a way that would permit privacy interests to advance in a manner that federal laws have thus far failed to do.

The tort of intrusion also applies to the disclosure of personal information.<sup>212</sup> The tort creates liability for the intentional intrusion upon another person's solitude, seclusion, or private affairs in a manner that would be highly offensive to a reasonable person.<sup>213</sup> The intrusion need not be physical; but can give rise to liability for the unauthorized prying into a bank account<sup>214</sup> or unwarranted access to a credit report.<sup>215</sup>

---

212. See, e.g., *Rodgers v. McCullough*, 296 F. Supp. 2d 895, 904 (W.D. Tenn. 2003) (alleging tort where the opposing attorney in a custody dispute used the plaintiff's credit report without a permissible purpose, acknowledging that Tennessee recognized the tort but ruling that a fact issue existed as to whether the use would have been highly offensive to a reasonable person). Not every state recognizes the tort of intrusion, however. See, e.g., *Hougum v. Valley Mem'l Homes*, 574 N.W.2d 812 (1998) (declining to decide whether tort of invasion of seclusion exists in North Dakota).

213. See *Phillips v. Grendahl*, 312 F.3d 357, 372 (8th Cir. 2002); *Olwell v. Med. Info. Bureau*, No. Civ. 01-1481 JRTFLN, 2003 WL 79035, at \*7 (D. Minn. Jan. 7, 2003); *Joseph v. J.J. Mac Intyre Cos., L.L.C.*, 238 F. Supp. 2d 1158, 1169 (N.D. Cal. 2002); *Bailer v. Erie Ins. Exchange*, 687 A.2d 1375, 1380, 1381 (1997); *Irvine v. Akron Beacon Journal*, 770 N.E.2d 1105, 1115 (Ohio Ct. App. 2002) (affirming jury's award of \$100,000 in punitive damages for defendant's repeated computer-dialed sales calls to plaintiff's home); see also *Remsburg v. Docusearch, Inc.*, 816 A.2d 1001, 1008 (2003); *Lovgren v. Citizens First Nat'l Bank*, 534 N.E.2d 987, 989 (1989) (declining to decide whether tort recognized in Illinois); *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998); *Household Credit Servs., Inc. v. Driscoll*, 989 S.W.2d 72, 84 (Tex. App. 1998); RESTATEMENT (SECOND) OF TORTS § 652B (1977).

214. See, e.g., *Lowe v. Surpas Resource Corp.*, 253 F. Supp. 2d 1209, 1239 (D. Kan. 2003) (deciding that it is for the jury to decide whether debt collector's actions intruded upon borrower's seclusion); *Pulla v. Amoco Oil Co.*, 882 F. Supp. 836, 867 (S.D. Iowa 1994) (affirming verdict that defendant had intruded upon the seclusion of plaintiff, who was defendant's employee, by accessing his credit card records to check his activities on days he had called in sick; rejecting defense that defendant had a legitimate objective in reviewing the records), *aff'd in part, rev'd in part on other grounds*, 72 F.3d 648 (8th Cir. 1995); *Remsburg*, 816 A.2d at 1008-09 (reasoning that people have a reasonable expectation that someone to whom they disclose their social security numbers will keep the numbers private, and therefore the wrongful disclosure of the number may be considered sufficiently offensive to support an action based on intrusion upon seclusion; however, people do not have a similar expectation of privacy as to their work addresses, and therefore no intrusion upon seclusion action can be based on the release of that information); *McGuire v. Shubert*, 722 A.2d 1087, 1092 (Pa. Super. 1998) (concluding that the defendants' acquisition of the plaintiffs' financial information could fulfill the intrusion tort). But see *Phillips*, 312 F.3d at 372 (future mother-in-law's improper purpose to obtain credit report on plaintiff did not render acquisition "highly offensive" for purposes of intrusion upon seclusion invasion of privacy tort); *In re Trans Union Corp. Privacy Litig.*, 211 F.R.D. 328, 343-42 (N.D. Ill. 2002) (consumer reporting agency's disclosure of plaintiffs' credit reports to target marketing firms did not meet highly offensive element of intrusion upon seclusion invasion of privacy claim); *Fabio v. Credit Bureau of Hutchison, Inc.*, 210 F.R.D. 688, 693-94 (D. Minn. 2002) (debt collector's use of curse words in telephone demands for payment did not render intrusion

Thus, the common law of torts offers a number of avenues to pursue those who breach privacy. However the torts, interpreted in a cramped and faded way, may insufficiently protect individuals from modern privacy invasions. Nonetheless, courts may continue to develop the torts to respond to the increased use of personal information in our society. Because of state torts' capacity for adaptation, federal statutes should minimize their interference in the evolution of those torts. HIPAA, which designates a floor of protection privacy but allows states to create standards even more protective of privacy, offers a model for minimal federal statutory intrusion on privacy protection by the states.<sup>216</sup>

## 2. *State Protection of Privacy through Enacted Laws*

State governments, similar to the federal government, have responded to modern threats to privacy with legislative action, and these statutes are much more likely than federal statutes to provide injured citizens with remedies. Just as the federal government has enacted the FCRA, HIPAA, and GLB, all to cope with the increasing availability and power of personal information, several state governments have similarly enacted legislation designed to target specific areas of privacy threats.

For example, a variety of states have enacted state credit reporting statutes to supplement the FCRA, statutes that provide for private enforcement.<sup>217</sup> As identity theft incidents have risen, states have enacted a number of statutes designed to deter identity theft and to help

---

highly offensive); *Cummings v. Walsh Constr. Co.*, 561 F. Supp. 872, 884 (S.D. Ga. 1983) (under Georgia law, tort requires physical invasion akin to trespass).

215. *Smith v. Bob Smith Chevrolet, Inc.*, 275 F. Supp. 2d 808, 822 (W.D. Ky. 2003) (denying defendant's motion for summary judgment).

216. 42 U.S.C. § 1320d-7(a)(2) (2006).

217. *See, e.g.*, ARIZ. REV. STAT. ANN. §§ 44-1691 to 44-1697 (2008); CAL. CIV. CODE §§ 1785.1-1787.3 (2008); COLO. REV. STAT. §§ 12-14.3-101 to 12-14.3-109 (2008); KAN. STAT. ANN. §§ 55-701 to 55-722 (2008); LA. REV. STAT. ANN. §§ 9:3571.1-3571.2 (2008); ME. REV. STAT. ANN. tit. 10, §§ 1311-1329; MD. CODE ANN. COM. LAW §§ 14-1201-1218 (2008); MASS. GEN. LAWS ANN. ch. 93, §§ 50-68 (2008); MINN. STAT. §§ 13C.001-13C.04; 72A.496-72A.505 (2008); MONT. CODE ANN. §§ 31-3-101 to 31-3-153 (2007) (expressly providing that a civil action for defamation, invasion of privacy or negligence is available against agencies that do not comply); NEV. REV. STAT. §§ 598C.010 to 598C.200 (2008); N.H. REV. STAT. ANN. §§ 359-B:1 to 359-B:21 (2008); N.J. STAT. ANN. §§ 56:11-28 to 56:11-41 (2008); N.M. STAT. ANN. §§ 56-3-1 to 56-3-8 (2008); N.Y. GEN. BUS. LAW §§ 380 to 380-t (2008); OHIO REV. CODE ANN. §§ 3904.01 to 3904.22 (2008); OKLA. STAT. tit. 24, §§ 81-86, 147-148 (2008); R.I. GEN. LAWS §§ 6-13.1-20 to 6-13.1-27 (2007); TEX. FIN. CODE ANN. §§ 391.001 to 391.002, 392.001 to 392.404 (2007); UTAH CODE ANN. § 70C-7-107 (2008); VT. STAT. ANN. tit. 9, §§ 2480a-2480g (2008); WASH. REV. CODE §§ 19.182.005 to 19.182.902 (2008).

victims remediate the damage of theft.<sup>218</sup> That so many states have done so reveals the interest states have in protecting their citizens from this technology-assisted crime. The theft of an individual's identity co-opts that person's image for use wholly outside his or her control and thereby reaches to the heart of individual personhood and dignity, damage that states have a strong interest in preventing. However, the FCRA explicitly preempts state laws in many areas that have recently drawn state legislatures' attention.<sup>219</sup> With respect to identity theft, the FCRA preempts states from enacting requirements for fraud alerts in consumer reports,<sup>220</sup> the blocking of information resulting from identity theft,<sup>221</sup> and the verification by credit card issuers of the identity of an applicant whose credit file has been contaminated by identity theft.<sup>222</sup> Accordingly, state statutes that seek to curb the dignity-destroying effect that identity theft has on victims' credit histories may well be rendered useless by the FCRA's preemption provisions.<sup>223</sup>

States have similarly adopted legislation to provide remedies for the sorts of privacy invasions envisioned by GLB, involving the use of nonpublic personal information by financial institutions. Following the passage of the Act, a number of states enacted their own financial information privacy acts.<sup>224</sup> As discussed above, Congress did not equip GLB with its own private enforcement mechanism, and courts have held that injured consumers do not have the right to enforce the Act themselves.<sup>225</sup> In adopting statutes similar to the federal act, however, many states explicitly provided that individuals whose information was disclosed or misused could in fact bring a suit to recover for the violation in civil court.<sup>226</sup>

---

218. See Fed. Trade Comm'n, Identity Theft State Laws, <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/laws.html> (listing the state identity theft laws by category).

219. See text accompanying notes 44 to 48, *supra*.

220. 15 U.S.C. § 1681t(b)(5)(B).

221. *Id.* § 1681t(b)(5)(C).

222. *Id.* § 1681t(b)(5)(B).

223. *Id.* § 1681t(b)(5)(B), (C). For instance, several states have developed security alert provisions similar to that of 15 U.S.C. § 1681c-1. See, e.g., CAL. CIV. CODE § 1785.11.1 (West 2008); 815 ILL. COMP. STAT. ANN. 505/2VV (West 2008); LA. REV. STAT. ANN. § 9:3568(C) (2008). Several states have also enacted provisions similar to that of 15 U.S.C. § 1681c-2, requiring consumer reporting agencies to block false credit history information that arises from identity theft. See, e.g., ALA. CODE § 13A-8-200 (2008); CONN. GEN. STAT. ANN. § 36a-699f (2008).

224. See, e.g., statutes cited *supra* note 85.

225. See, *supra* note 81.

226. See, e.g., HAW. REV. STAT. § 431:3A-503 (2008) (designating violation of state insurance information privacy act an unfair or deceptive trade act or practice); ILL. COMP. STAT. § 530/20 (West 2008) (designating violation of state Personal Information Protection Act an unlawful practice under the Consumer Fraud and Deceptive Business

States have also been much more willing to put teeth into their health information statutes. For example, several states permit a private cause of action for the disclosure of genetic information without the owner's consent,<sup>227</sup> a disclosure that HIPAA prohibits without providing any remedy.<sup>228</sup>

Finally, as discussed above, states have shown initiative in creating legislation to guard against the damage caused when the security of computerized personal information is breached.<sup>229</sup> By doing so, states have brought Justice Brandeis's words to life, becoming "laborator[ies]" for new legislation that addresses new risks brought on by technology.<sup>230</sup> Even in the absence of legislation, state attorneys general have pursued lax data security practices pursuant to state consumer fraud statutes.<sup>231</sup> All of these actions evince the interests states have in protecting their citizens' privacy by developing remedies for new wrongs, whether through evolution of the common law or by statutory enactment.

---

Practices Act); MICH. COMP. LAWS §§ 500.501-500.547 (2008); MINN. STAT. ANN. § 60A.982 (West 2008) (designating violation an unfair trade practice); NEB. REV. STAT. § 44-923 (2008) (designating violation an unfair trade practice); N.C. GEN. STAT. § 58-39-105 (2008) (providing remedy); OR. REV. STAT. ANN. § 746.680 (West 2008) (providing limited remedies, including equitable relief, for the wrongful use or disclosure of insurance information); TENN. CODE ANN. § 56-8-119 (2008) (specifically creating a private cause of action for the violation of the federal GLB pursuant to the state unfair or deceptive act or practice provision).

*But see* IDAHO CODE ANN. § 14-1334 (2008) (prohibiting violations of GLB, but expressly providing that no private cause of action was created); IND. CODE § 27-2-20-4 (2008) (expressly providing that enactment did not create a private right of action); N.D. CENT. CODE § 26.1-02-27 (2008) (expressly providing that nothing in the state's provision prohibiting violations of GLB will be construed to create a private cause of action); OKLA. REV. STAT. ANN. § 307.2 (West 2008) (same).

227. *See, e.g.*, ALASKA STAT. §§ 18.13.010-100 (2008) (permitting a private cause of action for actual damages along with statutory damages of either \$5000 or \$100,000 (§ 18.13.020)); CAL. INS. CODE § 10149.1 (West 2008); NEV. REV. STAT. ANN. § 629.101-629.201 (West 2008).

228. 45 C.F.R. § 164.502 (2008). This assumes that the genetic information would constitute protected health information. *Id.* § 160.103. *See also* Valentin Munoz v. Island Fin. Corp., 364 F. Supp. 2d 131, 136 (D.P.R. 2005); Johnson v. Parker Hughes Clinics, No. Civ.04-4130 PAM/RLE, 2005 WL 102968, at \*2 (D. Minn. 2005); Univ. of Colo. Hosp. v. Denver Publ'g Co., 340 F. Supp. 2d 1142, 1144-45 (D. Colo. 2004); Logan v. Dept. of Veterans Affairs, No. 02-701 (RJL), 2004 WL 3168183, at \*4 (D.D.C. July 28, 2004); Northwestern Memorial Hosp. v. Ass'n of Am. Physicians & Surgeons, Inc., 224 F. Supp. 2d 1115, 1129 (S.D. Tex. 2002); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1180 (D. Wyo. 2001).

229. *See, e.g.*, statutes cited *supra* note 90.

230. *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

231. *See, e.g., In re Eli Lilly, Inc., Assurance of Voluntary Compliance and Discontinuance*, available at <http://www.epic.org/privacy/medical/lillyagreement.pdf>.

C. *Federal Laws and the Tradition of Private Attorneys General*

As discussed above, the trend in federal privacy statutes has been to undercut the interests of individuals in protecting privacy rights. Not only does this approach diverge from that taken by states, it contrasts sharply with those federal statutes that permit enforcement through “private attorneys general.” Such parties can vindicate statutory policies, efficiently enforce congressional standards, deter socially harmful behavior, and offset any capture of governmental regulators by regulated parties. First used by Justice Jerome Frank in *Associated Industries v. Ickes*,<sup>232</sup> the term “private attorney general” refers to anyone who brings a proceeding to vindicate the public interest. Such a person can be a “powerful engine of public policy.”<sup>233</sup> Private causes of action help to enforce a variety of federal statutes, including antitrust, environment, securities fraud, consumer protection, and other federal legislation enacted to coerce private parties into acting for the benefit of the good, rather than for personal profit.<sup>234</sup>

Allowing private attorneys general to bring claims in court serves a highly efficient economic purpose of “addressing corporate misconduct without requiring a rigid government bureaucracy.”<sup>235</sup> Private suits can boost public enforcement, which is often constrained by limited funds, without burdening the taxpayers.<sup>236</sup> Where a federal law promotes important social norms or private incentives, enlisting private individuals to enforce those norms can achieve the same impact that, at the governmental level, could require many bureaucrats and much funding.<sup>237</sup>

In addition, and of great significance to privacy, where deterrence means much because privacy lost cannot be regained, the use of private attorneys general can deter actors from violating the set standards. Private litigation may obtain compensation for those injured by a violation of the statute, but may also deter law-breaking behavior by supplementing public enforcement efforts, thereby “multiplying the total resources committed to the detection and prosecution of the prohibited

---

232. *Associated Indus. v. Ickes*, 134 F.2d 694, 704 (2d Cir. 1943).

233. Jeremy A. Rabkin, *The Secret Life of the Private Attorney General*, 61 LAW & CONTEMP. PROBS. 179, 179 (1998).

234. See Abram Chayes, *The Role of the Judge in Public Law Litigation*, 89 HARV. L. REV. 1281, 1284 (1976).

235. Rustad, *supra* note 180, at 520.

236. See Trevor W. Morrison, *Private Attorneys General and the First Amendment*, 103 MICH. L. REV. 589, 608 (2005).

237. See Frederick Schauer & Richard H. Pildes, *Electoral Exceptionalism and the First Amendment*, 77 TEX. L. REV. 1803, 1831 (1999).

behavior.”<sup>238</sup> An actor who knows that interested private eyes, in addition to weary and overworked (and possibly uninterested) public ones, are supervising its acts, may find the risk of being caught sufficiently high to encourage the choice to conform to the legal standard.

Recognizing the benefits that a private enforcement provision can provide to the public, many states have incorporated them into their consumer protection and other, similar public interest statutes. States recognize that public enforcement alone may fail to fully motivate those regulated to comply with the statutory standard.<sup>239</sup> For example, California’s consumer protection statute has particularly broad remedial provisions, operating to “effectuate the full deterrent force” of that statute.<sup>240</sup> Private suits to enforce these statutory rights can in this way affect industry behavior far beyond the righting of the immediate plaintiff’s wrong.<sup>241</sup>

Despite these benefits, the collected federal privacy laws discussed above have in common that they discourage, if not outright eliminate, a role for private attorneys general. By refusing to allow private citizens to enforce all the rights conferred on them, Congress lost opportunities to give life to the policies embodied within those statutes.<sup>242</sup> In contrast, a private cause of action can help implement a two-pronged enforcement scheme, thereby providing a backup in the case of impotent agency action.<sup>243</sup>

Not only can private parties who have enforcement power supplement public enforcement efforts, but private parties also can enforce the social norms embodied in federal statutes when government

---

238. John C. Coffee, Jr., *Rescuing the Private Attorney General: Why the Model of Lawyer as Bounty Hunter Is Not Working*, 42 MD. L. REV. 215, 218, 221-23 (1983) (noting concern that the mechanism of private attorneys general has been abused, notwithstanding the deterrent function, and empirical evidence that too many private actions have simply “piggyback[ed] onto public enforcement efforts”).

239. See Morrison, *supra* note 236, at 605-06 (noting that many state environmental and consumer protection laws provide for citizen suits).

240. Fletcher v. Sec. Pac. Nat’l Bank, 591 P.2d 51, 57 (Cal. 1979).

241. See Morrison, *supra* note 236, at 607 (“Legislatures, in short, have often commissioned private plaintiffs in the pursuit of the public interest.”).

242. Rustad, *supra* note 180, at 529 (citing Chayes, *supra* note 234).

243. As the Supreme Court has said in the context of *qui tam* actions:

[O]ne of the least expensive and most effective means of preventing frauds on the Treasury is to make the perpetrators of them liable to actions by private persons acting, if you please, under the strong stimulus of personal ill will or the hope of gain. Prosecutions conducted by such means compare with the ordinary methods as the enterprising privateer does to the slow-going public vessel.

United States ex rel. Marcus v. Hess, 317 U.S. 537, 541 n.5 (1943) (quoting United States v. Griswold, 24 F. 361, 366 (D. Or. 1885)).

regulators and legislators are unwilling to confront large industry players despite the damage they may be doing to individuals.<sup>244</sup> As noted by proponents of private attorneys general, they help to ensure that enforcement of statutory norms is “not wholly dependent on the current attitudes of public enforcers,”<sup>245</sup> an effect also known as “capture.”<sup>246</sup> Where a public regulatory agency has a monopoly on enforcement, there is a high risk that those the agency is charged with regulating may have far more influence over the agency than those the agency is charged with protecting.<sup>247</sup> That is, “the agency might become unduly influenced by the entities it regulates.”<sup>248</sup> That the Department of Health and Human Services has been reluctant to exact penalties for the violations of HIPAA’s privacy provisions does not indicate the absence of such influence by those who are to abide by the act’s protections.<sup>249</sup>

Without a private right of enforcement, private attorneys general cannot serve the functions of enforcing standards, deterring misconduct, and supplementing governmental enforcement. The statutes may well result in *de facto* immunity for reprobate industry members who profit and thrive on invading the privacy of individuals. Depending on federal agencies to enforce the rights of private citizens is costly and depends too much on those agencies being willing to confront potentially powerful businesses that can exert pressure to minimize the ultimate effects of such actions. By denying injured individuals any right to enforce their privacy interests, Congress loses an opportunity to “permit ordinary citizens to change corporate practices,” a major purpose of the social policy of torts.<sup>250</sup>

### III. A RETURN TO STATE ENFORCEMENT

To be meaningful, to alter behavior, and to promote asserted values, rights require remedies.<sup>251</sup> Without remedies, only the good wishes of

---

244. See Rustad, *supra* note 180, at 520.

245. Coffee, *supra* note 238, at 227.

246. See Morrison, *supra* note 236, at 609.

247. *Id.* See also Einer R. Elhauge, *Does Interest Group Theory Justify More Intrusive Judicial Review?*, 101 YALE L.J. 31, 42 (1991) (collecting literature on agency capture); Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1669, 1713 (1975) (“It has become widely accepted, not only by public interest lawyers, but by academic critics, legislators, judges, and even by some agency members, that the comparative overrepresentation of regulated or client interests in the process of agency decision results in a persistent policy bias in favor of these interests.”) (citations omitted).

248. Morrison, *supra* note 236, at 609.

249. See text accompanying notes 136 to 141, *supra*.

250. Rustad, *supra* note 180, at 527.

251. See text accompanying notes 159 to 179, *supra*.

the regulated will motivate them to comply with statutory demands,<sup>252</sup> and where compliance would cut into profits or inhibit competitive goals, such good wishes will not suffice. As privacy rights have moved from state to federal dominion, remedies have been lost. Congress has adopted standards but has crippled the ability of individuals hurt by the breach of those standards to recover for the breach. While Congress empowered federal and state agencies with enforcement, these agencies have not embraced their responsibility to pursue violators. A variety of reasons may account for this—insufficient personnel and resources, lack of institutional will, and political pressure are leading candidates. Regardless of the reasons, federal privacy laws as implemented have left consumers more, not less, vulnerable, and have given more, not less, power to the entities that have access to individuals' personal data.

Given the impotency of these federal laws, we should construe narrowly whatever power they may have to supplant state privacy laws. In addition to helping individuals obtain redress for violated rights, such constraint would also fulfill a signaling function to alert states that their efforts to address the injuries that can arise with the abuse of new technology would not be for naught. This would encourage state legislatures and courts to fulfill the opportunity to “experiment” in their laws, and to evolve to adjust to changing circumstances as tort law traditionally has.<sup>253</sup> In responding to such a signal, states may adapt old torts to the changing threats to privacy or initiate new torts.<sup>254</sup> Alternatively, states can bypass the common law entirely and provide relief through legislation.

Allowing states to participate in protecting privacy would provide the benefit of multiple levels of government, where “if one fails to act, another can step in to solve the problem.”<sup>255</sup> This would allow states to develop their own laws “in accordance with justice and humanity.”<sup>256</sup>

---

252. See Ziegler, *supra* note 158, at 678.

253. *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

254. See Betsy J. Grey, *The New Federalism Jurisprudence and National Tort Reform*, 59 WASH. & LEE L. REV. 475, 514 (2002) (offering examples of significant new torts that states have created to address new circumstances, including the tort of invasion of privacy). The author also notes that those situations, such as in the Fair Credit Reporting Act, *see* text accompanying notes 42 to 48, *supra*, where the congressional legislation has voided state common law remedies without substituting a corresponding federal remedy, invokes high state interest that justifies greater scrutiny of the preemption provision. *Id.* at 536.

255. Erwin Chemerinsky, *Empower States: The Need to Limit Federal Preemption*, 33 PEPP. L. REV. 69, 74 (2005).

256. *Baltimore & O.R. Co. v. Baugh*, 149 U.S. 368, 411 (1893) (Field, J., dissenting) (noting differences among court decisions on the fellow servant rule that allowed

As discussed above, however, the trend in federal privacy law has been to minimize potential remedies. Congress does this by failing to provide for a private cause of action, by limiting the monetary value of available remedies, and by preempting states from enacting legislation that could protect privacy.

A. *State Tort Law*

Privacy standards have a natural home in tort. As discussed above, torts, especially at common law, provide a number of societal benefits. Among these benefits is deterrence. Ideally, the risk of uncertain damages, and especially punitive damages, deters those who would otherwise ascertain advantages from engaging in the discouraged behavior. The deterrent effect is most valuable for privacy invasions. Once digitalized and released, information can be copied, emailed, aggregated, and archived—a genie that cannot be rebottled.

In addition, enforcement of standards through the judicial process helps to interpret and define those standards, which notifies the benefited of what they can expect from the restricted, and notifies the restricted of how they should constrain their behavior in order to avoid liability. Aside from the notice function, the judicial process can also incorporate changes in technology and in societal norms by responding to individual sets of circumstances.

To the extent that a federal statute supplants state laws, such deterrence, notice, and adaptation benefits are lost, unless enforcement at the federal level mimics what would have been achieved at the state level. Where remedies are minimized or removed entirely, however, the federal law becomes not much more than a “hope or a wish.”<sup>257</sup>

The standards held hostage by federal privacy laws should be enforceable by the states because people value the types of privacy that the laws purport to protect.<sup>258</sup> Social norms are reflected in Congress’s own statements and actions.<sup>259</sup> They are echoed in statements by agencies, such as the Department of Health and Human Services’ that declared that medical privacy is a “fundamental right” different from

---

corporations to be exempt from liability for the negligence of employees where that negligence injured another employee).

257. Ziegler, *supra* note 158, at 678.

258. See RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 227-29 (1989) (discussing types of information that people want to shield).

259. See, e.g., H.R. REP. NO. 104-496, at 103 (1996), as reprinted in 1996 U.S.C.A.N. at 1865, 1868 (noting the purpose of HIPAA).

“ordinary economic good[s],”<sup>260</sup> and described “the inherent meaning of privacy: it speaks to our individual and collective freedom.”<sup>261</sup>

To protect privacy is to recognize the fundamental dignity of individuals, that each has a unique personality that the individual can develop and express only within a zone of privacy. To immunize actors from consequences for any violation of privacy, to deprive those injured of any sort of remedy for that violation, risks undermining the very attributes that the tort of privacy law is designed to protect—dignity and personality. Common law privacy torts recognize the value of human dignity by encouraging the circumstances “necessary for individuation—the realization of one’s distinctive identity as a unique human being.”<sup>262</sup> Such torts can help protect the integrity of individual identity, “man’s spiritual nature.”<sup>263</sup>

Enhancing enforcement of privacy standards can confer societal benefits in addition to individual ones. Avishai Margalit describes a civilized society as one whose members do not humiliate one another, and a decent society as one in which institutions do not humiliate people.<sup>264</sup> A healthy respect for privacy can help move a society to become both civilized and decent. Given the withdrawal of remedies at the federal level, states should step in to promote individual dignity by protecting privacy.

### B. *State Enacted Legislation*

State-enacted laws can also add meaning to the privacy standards set by Congress. In tort law, states have historically led the way in developing causes of action to accommodate society’s changes.<sup>265</sup> Sometimes, the federal government has, through a statute, established new standards that states have then used to follow up with their own legislation, especially for consumers. For example, Congress amended the Federal Trade Commission Act in 1938 to specifically prohibit “unfair or deceptive acts or practices.”<sup>266</sup> However, the Federal Trade Commission Act did not create a private cause of action, but merely

---

260. Preamble to the Privacy Rule, 65 Fed. Reg. 82,462, 82,464-65 (Dec. 28, 2000).

261. *Id.*

262. Kahn, *supra* note 113, at 404 (2003). Professor Kahn recognizes that the relationship of personhood, dignity, and privacy is complex, and describes it as follows: “[w]hereas dignity broadly implicates a consideration of the inherent value of human beings, privacy involves the more focused right to protect the conditions necessary to individuation. That is, where dignity broadly conceived is a condition of personhood, privacy is an attribute of individuality.” *Id.* at 378.

263. Warren and Brandeis, *supra* note 99, at 193.

264. Avishai Margalit, *THE DECENT SOCIETY* 201-22 (1996).

265. *See supra* notes 180 to 204 and accompanying text.

266. 15 U.S.C. § 57a (2006).

empowered the Federal Trade Commission to seek relief.<sup>267</sup> To fill the void, states enacted their own consumer protection legislation, and now every state except Iowa encourages consumers to supplement the efforts of public actors, or state agencies, to enforce the law by permitting individuals to bring suits themselves.<sup>268</sup> In many cases these new statutes essentially supplant the traditional common law action for fraud.<sup>269</sup> An advantage of common law fraud is that it offers the opportunity for punitive damages.<sup>270</sup> Many states sought to retain that benefit by adding their own punitive or treble damages provisions,<sup>271</sup> a feature that has been described as essential to their mission.<sup>272</sup> Through enhanced remedial provisions these state statutes can deter harmful behavior, realizing the norms that the statutes value.

The personal information security statutes, discussed above,<sup>273</sup> are a fresh example of the sorts of initiatives that state legislatures can take, with all of the alacrity missing at the federal level. Rather than seeking to preempt such legislation with a toothless substitute, the federal government should recognize the benefits to individuals' privacy and well-being that such measures can provide.

Privacy, in particular, may be better suited to state law because of the difficulty in reaching agreement on what privacy is. Willis Ware has argued that for purposes of policy making, we should stop trying to agree on what privacy is and instead develop a consensus on what an "invasion" of privacy is.<sup>274</sup> Without interference from the federal government of the sort described above, states would be free to

---

267. See generally *Holloway v. Bristol-Myers Corp.*, 485 F.2d 986 (D.C. Cir. 1973) (discussing history of the FTC Act and the reasons why a private remedy should not be recognized).

268. See National Consumer Law Center, *UNFAIR AND DECEPTIVE ACTS AND PRACTICES* § 7.2.1 (6th ed. 2006).

269. But see *id.* § 9.6.3 (identifying advantages of common law deceit and other tort actions over statutory deceptive practices act actions).

270. *Id.*

271. Ten states have deceptive practices statutes that authorize punitive damages directly. CAL. CIV. CODE. § 1780 (2008); CONN. GEN. STAT. § 42-110G (2008); D.C. CODE ANN. § 28-3905(K)(1)(C) (LexisNexis 2008); GA. CODE ANN. § 10-1-399 (2008); IDAHO CODE § 48-608 (2008); KY. REV. STAT. § 367.220 (2008); MO. REV. STAT. § 407.025 (2008); OR. REV. STAT. § 464.638 (2008); R.I. GEN. LAWS § 6-13.1-5.2 (2008); VT. STAT. ANN. tit. 9, § 2461 (2008). Many more authorize treble damages.

272. Steven W. Bender, *Oregon Consumer Protection: Outfitting Private Attorneys General for the Lean Years Ahead*, 73 OR. L. REV. 639, 671-72 (1994).

273. See *supra* notes 229 to 231 and accompanying text.

274. Willis A. Ware, *A Taxonomy for Privacy*, in REPORT ON THE NATIONAL SYMPOSIUM ON PERSONAL PRIVACY AND INFORMATION TECHNOLOGY 16 (1981); see James P. Nehf, *Incomparability and the Virtues of Ad Hoc Privacy*, 76 U. COLO. L. REV. 1, 43 (2005) (arguing that using such an approach "tracks and reflects usage of evolving technologies as society adapts to new intrusions and adjusts the boundaries of acceptable conduct, rather than a priori prescribing those boundaries").

experiment with standards that reflect a more protective attitude toward personal information. They could, for example, model many European nations that reject the presumption that personal information should be freely available for commercial exploitation.<sup>275</sup>

#### CONCLUSION

Federal privacy statutes engage in a game of deception. They purport to solidify norms for the privacy of our personal information, whether financial, medical, or other. They make demands of those who have control over individual information. However, they often fail to offer real remedies when those demands are not met, and sometimes even invalidate state measures meant to protect privacy. As a consequence, while those whom the federal laws purport to protect may falsely perceive that the disclosure of their private data will be punished, the regulated receive comfort that they can breach privacy with impunity. This trend of toothlessness in federal privacy law began with the Fair Credit Reporting Act, which allows some, but not complete, private remedies, and has continued through the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act. Most recently, the trend appears in bills offered to protect the security of personal information data that also prohibit private remedies otherwise existent in state laws and furthermore preempt those state laws.

While federal laws offer some hope by allocating the responsibility for enforcement to agencies and states, limiting enforcement to governmental agencies may be little better than eliminating enforcement entirely. Such agencies have shown insufficient appetite for taking powerful institutions to task. In effect, agencies depend on regulated institutions to police themselves, but too much profit can be had from the abuse of privacy to count on the good will of those that have power over personal information.

Federal laws undercut the potential for redress by limiting private causes of action, and by sometimes simultaneously preempting state protections. However, given the importance of privacy norms and the tradition of rights and remedies for privacy at the state level, states should seek to push their capacity to use laws, whether common or enacted, to protect their citizens to the very limits they can. The dearth of federal remedies contradicts a long tradition of rights and remedies, and is at fundamental odds with the policy of law serving to crystallize

---

275. See Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L. J. 461, 469 (2000); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 13-14 (1996).

2008]

A DEARTH OF REMEDIES

53

and promote social norms. Although other federal laws protecting individuals have encouraged such promotion by allowing private attorneys general, federal privacy laws have broken with this tradition where they have sought to eliminate any private remedy.

Enforcement of social privacy norms, as embodied in laws state or federal, is necessary to meaningfully protect personality and dignity. States can resume their traditional roles as protectors of their citizens by responding to increased threats to privacy. They can do this by adapting common law torts or by enacting legislation; where these instruments provide enforcement through private causes of action, those protected by the instruments can vindicate their rights. More importantly, such remedies can deter violations to begin with, the ultimate aim of any privacy provision.