2010

Reunifying Privacy Law

Lior Strahilevitz

Reunifying Privacy Law

Lior Jacob Strahilevitz†

In the years since Samuel Warren and Louis Brandeis proposed a unified theory of invasion of privacy tort liability, American information privacy law became increasingly fragmented and decreasingly coherent. William Prosser's 1960 article, Privacy, which heavily influenced the Restatement of Torts, endorsed and hastened this trend toward fragmentation, which spread from tort law to the various statutory branches of information privacy law. This Article argues for the reunification of information privacy law in two connected ways. First, Prosser's fragmented privacy tort should be replaced with a unitary tort for invasion of privacy that looks to the private or public nature of the information, the degree to which a defendant's conduct violates existing social norms, and the social welfare implications of the defendant's conduct. Second, the reunified common law of torts should become the model for judicial interpretation of various other branches of information privacy law, such as the Freedom of Information Act's privacy provisions, the Privacy Act, and the constitutional right of information privacy. The Article examines how this reunification project can be accomplished, why it is desirable, and whether it is consistent with the U.S. Supreme Court's methodological guidance in privacy controversies.

The final section of the Article argues that the pending Supreme Court case of NASA v. Nelson is an ideal vehicle for pushing the law of information privacy back toward its relatively coherent and unified origins. Nelson will be the first Supreme Court case in thirty-three

† Deputy Dean and Professor of Law, University of Chicago Law School. Thanks to Ryan Calo, Sherry Colb, Rosalind Dixon, Lee Fennell, Tom Ginsburg, Tom Gorman, Mike Hintze, Aziz Huq, Avner Levin, Saul Levmore, Richard McAdams, Martha Nussbaum, Paul Ohm, Jennifer Rothman, Adam Samaha, Paul Schwartz, Kathy Strandburg, David Strauss, Matt Tokson, Eugene Volokh, Felix Wu, and faculty workshop participants at the University of Chicago Law School and Cornell Law School, as well as participants in U.C. Berkeley's "Prosser's *Privacy* at Fifty Symposium" and the Privacy Law Scholars Conference for comments on earlier drafts, Katie Heinrichs and Smitha Nagaraja for research assistance, and the Morton C. Seeley Fund and Milton and Miriam Handler Foundation for research support.

years to confront squarely the question of whether the Constitution protects a right to information privacy apart from the Fourth Amendment context. Because the common law tort cause of action and constitutional action involve similar harms and considerations, it is appropriate to reconcile the presently divergent doctrines, though this could be done in one of two ways. The most sensible approach to reunification is to conclude, as the Sixth Circuit has, that there is no such thing as a constitutional right to information privacy, and that such rights are appropriately vindicated via statutory remedies. An alternative approach would be to recognize the existence of a constitutional right, as most circuit courts have, but to hold that the elements of a constitutional violation mimic those associated with the reunified privacy tort.

Introduction 2008
I. Posner Versus Prosser 2012
II. The Constitutional Right to Information Privacy 2015
III. FOIA Jurisprudence and Reunification 2020
IV. Disclosure Under the Privacy Act 2024
V. A Framework for Reunifying Privacy Law 2032
VI. The Desirability of Coherence in Privacy Law 2036
VII. Can *Nelson* Follow *Maynard*? 2038

INTRODUCTION

In 1949, Germany was divided into two countries, East and West. Forty years later, the Berlin Wall fell, and Germany was reunified a year after that.

In 1960, William Prosser wrote an enormously influential article dividing the law of privacy into four components: intrusion, public disclosure, appropriation, and false light. Fifty years later, American privacy law has become far more fragmented than it was in Prosser's era.

We cannot lay all the blame for privacy law's fragmentation upon Prosser. Privacy case law hardly seemed coherent when Samuel Warren and Louis Brandeis found it. By the time they finished describing it, however, the law of privacy fit together rather elegantly, which is part of what made their article so important. Over the next several decades, courts began to embrace, in fits and starts, their coherent vision of what the law could be. Yet there were always cases that rejected their vision or, worse still, made a mess out of Warren-and-Brandeis principles that the judges claimed to embrace. Prosser was the first scholar to emphasize privacy law's fragmentation, and he lent it his influential stamp of approval. Some contemporaries opposed his argument for

fragmentation,[1] but it was Prosser who prevailed. Fifty years ago, Prosser began in earnest a process of fragmentation that would create great internal inconsistency in this body of law. Prosser's revolution in tort law preceded the enactment of ad hoc privacy statutes that neither fit together, nor aligned with the newly fragmented common law in a coherent way. We might suspect that the common law fragmentation influenced the subsequent statutory fragmentation, while recognizing that it would be unfair to lay at Prosser's feet all of the blame for the mess that information privacy doctrine has become.

The division of Germany was not inexplicable. It resulted from tactical decisions made by generals and politicians during the Second World War, the power politics of the day, and the onset of the Cold War. But Germany's division was irrational and unfortunate. Germans were united by a common language, culture, history, system of governance, and by their collective culpability for twentieth-century atrocities. Two Germanies did not represent a stable equilibrium.

Nor was the fragmentation of American information privacy law inexplicable—it was merely irrational. It has left us with a body of case law whose contradictions are sometimes apparent, but often subtle. It is time to move aggressively toward the reunification of American information privacy law. This Article makes the case for returning the law to its 1890 origins—to an era in which the law was sparse but coherent. I argue that the Supreme Court has been directing the lower courts toward the reunification project, though in ways subtle enough to have gone largely unnoticed by the lower courts. In a presently pending case, the Court has a golden opportunity to be much more blatant about endorsing the goal of returning coherence to information privacy law, and this Article concludes by examining the two ways in which the Court can decide *NASA v. Nelson* in a manner that promotes privacy law's reunification.

Before turning to the case law in earnest, I do want to say a word about the scope of my argument. I am not advocating here the unification of information privacy and decisional privacy doctrine. Though some scholars have argued that the *Griswold* line of cases shares important commonalities with information privacy law,[2] I believe the stark differences in the respective analytical frameworks, stakes, historical pedigrees, and distributive contexts

1. See, for example, the eloquent anti-fragmentation article, Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964). Bloustein argued that, by separating the unified invasion of privacy cause of action into four torts, Prosser undermined the important conceptual work that Warren and Brandeis had done. He also argued, contrary to Prosser, that a single societal interest—that of human dignity—undergirded all invasion of privacy claims.

2. An inventive and well-executed example of scholarship in this vein is Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006). An embarrassingly muddled and misguided example of this sort of scholarship is Lior Jacob Strahilevitz, *Consent, Aesthetics, and the Boundaries of Sexual Privacy After* Lawrence v. Texas, 54 DEPAUL L. REV. 671 (2005).

dwarf the extant similarities between informational and decisional privacy. Certainly, the differences are sufficient to warrant caution about the value of trying to unify these disparate strands. At the same time, the Article also accepts the argument, put forward at great length elsewhere, that information privacy itself is a category with enough commonalities to render it a coherent concept.[3]

The Article proceeds in seven parts. Part I argues for reunification within privacy tort law itself. It argues that it was unnecessary for Prosser to divide Warren and Brandeis's invasion of privacy tort into separate causes of action for intrusion upon seclusion and public disclosure of private facts. By fragmenting the tort, Prosser and the Restatement robbed it of some of its intuitive appeal. Perhaps as a result, courts sometimes subconsciously push back against the Prosserian framework, and jumble together the elements of the distinct tort.

Part II and subsequent parts advocate the reunification of privacy law across doctrinal domains. Part II opens the broader case for reunification by suggesting that the constitutional right to information privacy sometimes overlaps substantially with privacy tort law. It is therefore a genuine puzzle why the two overlapping causes of action should have divergent elements. While there are some jurisdictions in which sovereign immunity and state tort claims acts preclude the possibility of a suit against the state for invasion of privacy harms, and that is largely true of the federal government because of "due care" and "discretionary function" immunity under the Federal Torts Claims Act, it is difficult to construct a persuasive case for why the Constitution—as opposed to ordinary legislation—is the appropriate avenue for providing plaintiffs with relief.

Part III advocates the reunification of privacy tort law with Freedom of Information Act (FOIA) privacy law. It shows that, while the Supreme Court lacked a compelling justification for holding that "unwarranted invasions of personal privacy" could have very different meanings in the FOIA and tort contexts, the Court's most recent decision has suggested that it is appropriate to look to privacy tort law to define an invasion of privacy under FOIA.

Part IV shows how to reconcile the Privacy Act with other aspects of information privacy law. It offers a new defense of the Supreme Court's leading privacy precedent, *Doe v. Chao*.[4] The Article suggests that while *Chao*'s reading of the pertinent statutory language is somewhat strained on its own terms, the decision may ultimately improve Privacy Act jurisprudence. The *Chao* decision inoculates the government against a significant threat posed by lower court decisions interpreting the Privacy Act in a manner that would

3. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM (1967); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

4. 540 U.S. 614 (2004).

impose substantial liability on the government even for disclosing information already readily accessible to the public. *Chao* also suggests that tort law principles should color judicial interpretation of the Privacy Act itself, providing the Court's most emphatic nudge in the direction of the reunification project.

Part V proposes the replacement of Prosser's two primary privacy torts with a single tort closer to what Warren and Brandeis envisioned. A unified tort with three essential elements—privacy, highly offensiveness, and negative effects on social welfare—offers a sensible analytical framework for analyzing privacy harms involving publication or intrusion. The Part then suggests that a reunified privacy tort might have an easier time grappling with the new privacy problems being presented by novel technologies.

Part VI offers three reasons why the reunification of information privacy law is desirable. More coherent law will lower the compliance costs faced by firms and individuals, improve the quality of common law adjudication by reducing uncertainty about how the law will treat particular controversies, and help equalize the treatment of similarly situated parties.

Part VII concludes with the timeliest part of the Article. In October, the Supreme Court heard oral argument in its first constitutional right to information privacy case in thirty-three years. This Part brings to bear the analysis from the previous parts of the Article to show how *NASA v. Nelson* can become a vehicle for accelerating the rationalization and reunification of privacy law. Given the mess that the lower courts have made of constitutional right to information privacy doctrine, there are two viable paths for the Court to take. The first approach would enhance coherence in privacy law by holding that there is no such thing as a constitutional right of information privacy, finding instead that the problems confronted in this category of cases are most appropriately dealt with via garden variety tort or statutory remedies. The second approach would regard the constitutional right to information privacy as a gap-filler where political pathologies prevent legislative processes from adequately vindicating privacy interests. If the constitutional right to information privacy is to persist, it ought to more closely resemble privacy tort law—and focus on the same three questions that are most relevant to tort liability: whether the information is private, what the applicable social norms are, and what social interests are vindicated by privacy and the absence of privacy. For reasons explained in the Article, the first path seems more attractive than the second, which in turns seems far superior to the continued development of a *sui generis* constitutional right of information privacy.

I.
POSNER VERSUS PROSSER

Let us begin with torts and the two most influential pieces of American privacy scholarship. In their 1890 article, *The Right to Privacy*,[5] Samuel Warren and Louis Brandeis described an undifferentiated cause of action for interference with one's right to be let alone. Some of the examples they used in their seminal article described the aggregation of information about individuals, while some focused on the dissemination of said information.[6]

The authors did not distinguish between these two kinds of cases. Tellingly, in a section of the article highlighting the limitations that had to be imposed on tort liability for invasion of privacy, they embraced categorical limitations. For example, if the cause of action for invasion of privacy came into conflict with the people's right to receive information about matters of legitimate public concern, privacy interests had to give way.[7]

Fast forward seven decades: William Prosser, writing the second seminal article on American privacy law, breaks the privacy torts into four components, reasoning, plausibly, that distinct considerations animate the questions of when information gathering and information publishing should be actionable, to say nothing of the differences between the publication of true versus false information and commercial versus noncommercial speech.[8] The two torts that receive the lengthiest treatment in Prosser's *Privacy*, and which seem most closely tied to privacy itself, are intrusion upon seclusion and public disclosure of private facts.[9] Although one tort deals with information gathering and the other deals with information dissemination, the public disclosure tort largely circumscribes the intrusion tort. If a defendant has engaged in public disclosure of private facts, the odds are quite high that either the defendant or the defendant's confederates have engaged in an intrusion upon seclusion. There will be occasional exceptions to this rule of thumb, such as where the plaintiff has voluntarily disclosed information to the defendant, who has disseminated it without a legal basis for doing so.[10]

The claim that public disclosure generally circumscribes intrusion upon seclusion is evident from an examination of the elements of the two torts. Under the Restatement, intrusion upon seclusion requires (1) an intentional intrusion into the (2) private affairs of another person, (3) in a manner highly

5. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

6. *Id.* at 295–96, 201–02.

7. *Id.* at 215.

8. *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

9. I do not address the misappropriation or false light torts here because I believe they have rather little in common with either the two other privacy torts or the other bodies of information privacy law considered herein.

10. *See, e.g.*, Trammell v. Citizens News Co., 148 S.W.2d 708 (Ky. Ct. App. 1941).

offensive to a reasonable person.[11] The public disclosure tort typically requires (1) intentional disclosure by the defendant to the public,[12] (2) of private facts or affairs concerning another person, (3) in a manner highly offensive to a reasonable person and (4) not of legitimate public concern.[13] If a fact is private for the purposes of the intrusion tort, it is private for the purposes of the public disclosure tort, and vice versa. Along the same lines, the "highly offensive" nature of the defendant's conduct must be manifest in either tort. Per Prosser, the courts are to focus on the offensiveness of the information gathering in the intrusion context and the information dissemination in the public disclosure context, though this fine distinction often eludes them.

Notice that Prosser's public disclosure of private facts tort requires two elements that are absent in the intrusion tort: publicity and non-newsworthiness. An intrusion upon seclusion is not dependent on the defendant sharing private information with anybody else. There are cases in which the plaintiff recovers even though the defendant is the only person who was shown to have learned the private information.[14] But cases in which there is an intrusion upon seclusion by one or two people, and no subsequent publicity, are rarely brought because the damages resulting from such harm are usually low.

Non-newsworthiness ostensibly provides the most salient difference between public disclosure and intrusion. When judges call a disclosure non-newsworthy, they mean to say that it has no social value—an equivalence that has become part of the doctrine.[15] If the defendant publicizes newsworthy information, then the plaintiff cannot recover for public disclosure, but if the defendant gathers newsworthy information, the plaintiff might be able to prevail on an intrusion claim. This critical distinction is part of black letter doctrine,[16] but it is not necessarily followed in practice.

---

11. RESTATEMENT (SECOND) OF TORTS § 652(B) (1977).

12. Some jurisdictions contravene the Restatement by recognizing negligent invasions of privacy, both via intrusion upon seclusion and public disclosure of private facts. *Compare* Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702 (D.C. 2009) (no negligent invasion of privacy liability), *and* Hudson v. S.D. Warren Co., 608 F. Supp. 477, 481 (D. Me. 1985) (no negligent invasion of privacy liability), *and* Bailer v. Erie Ins. Exch., 687 A.2d 1375, 1380–81 (Md. Ct. App. 1997) (no negligent intrusion liability), *with* Spinks v. Equity Residential Briarwood Apartments, 171 Cal. App. 4th 1004, 1043 (Cal. Ct. App. 2009) (no distinction between intentional and negligent invasion of privacy), *and* Prince v. St. Francis–St. George Hosp., 484 N.E.2d 265, 268–69 (Ohio Ct. App. 1985) (same). Texas law is currently split over whether negligent invasion of privacy claims are permitted. *See* Doe v. Mobile Video Tapes, Inc., 43 S.W.3d 40, 53 (Tex. App. 2001).

13. RESTATEMENT (SECOND) OF TORTS § 652(D) (1977).

14. *See, e.g.*, Hamberger v. Eastman, 206 A.2d 239, 242 (N.H. 1964).

15. *See, e.g.*, Capra v. Thoroughbred Racing Ass'n, 787 F.2d 463, 464 (9th Cir. 1986) (citing the newsworthiness factors as "the social value of the facts published" plus two other factors that go more to the strength of the plaintiff's privacy interest).

16. *See, e.g.*, Shulman v. Group W Prods., Inc., 955 P.2d 469, 493–94 (Cal. 1998); Mitchell v. Baltimore Sun, 883 A.2d 1008, 1023–24 (Md. Ct. App. 2005).

Arguably the most famous pair of American privacy tort law opinions is the Ninth Circuit's 1971 opinion in *Dietemann v. Time* and the Seventh Circuit's 1995 opinion in *Desnick v. ABC.*[17] In the privacy casebooks, Daniel Solove and Paul Schwartz prominently pair the cases side by side, and Anita Allen also compares them early in her casebook, though she devotes more space to *Dietemann.*[18]

The cases involve similar facts. In *Dietemann*, undercover reporters entered the home of a quack faith healer, gaining entry after telling Dietemann that he had been recommended by a friend of his, the fictitious "Mr. Johnson." Once inside, one of the journalists claimed to have a lump in her breast. Dietemann purported to diagnose her ailment and treat it using various gadgets. While Dietemann did not charge his patients as a matter of course, he did accept contributions in return for his services. Dietemann was later arrested for practicing medicine without a license and, in light of the photographs and recordings made by the reporters, pled nolo contendere in the criminal proceedings that preceded the tort action.[19]

Desnick involved journalists who hired actors to seek treatment in the clinics of Dr. Desnick, an ophthalmologist. The actors' interactions with medical personnel in the clinics were filmed surreptitiously. Although the actors were perfectly healthy, Desnick's clinics recommended that several of them undergo cataract surgery.[20] The broadcast of the ABC story on Dr. Desnick's practices evidently contributed to his leaving the profession.[21]

In *Dietemann*, the court held that the journalists for *Life* magazine had invaded Dietemann's privacy. Not surprisingly, then, Desnick's lawyers relied heavily on *Dietemann* in the Seventh Circuit. Writing for the court, Judge Posner conceded the similarities, noting that Dietemann's home doubled as his office and "[t]he parallel to this case is plain enough, but there is a difference. Dietemann was not in business, and did not advertise his services or charge for them. His quackery was private."[22] Such analysis is not a satisfying basis for distinguishing the case. Dietemann may have been less successful than Desnick, but both were in the same business. Dietemann just had a different business model: word of mouth advertising instead of billboards and print ads (a sensible decision, given that Dietemann's business was illegal), and the

17. Desnick v. ABC, Inc., 44 F.3d 1345 (7th Cir. 1995); Dietemann v. Time, Inc. 449 F.2d 245 (9th Cir. 1971).

18. ANITA L. ALLEN, PRIVACY LAW AND SOCIETY 47–50 (2007); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 84–89 (3d ed. 2009).

19. *Dietemann*, 449 F.2d at 245–47.

20. *Id.*

21. Marilynn Marchione, *Desnick Fined, Gives up Right to Practice for 2 Years*, Milwaukee J., April 8, 1995.

22. *Desnick*, 44 F.3d at 1353.

Radiohead "pay what you want" business model instead of fixed prices.[23] Coffee shops sometimes charge customers whatever they say they are willing to pay, but businesses they remain.[24] The differences between *Dietemann* and *Desnick* are simply matters of degree.

In trying to provide a defense for Judge Posner's treatment of Dietemann, my privacy law students almost invariably arrive at a pragmatic point with which Posner presumably would sympathize, and which is suggested by early portions of his opinion, especially its charming discussion of restaurant critics.[25] Desnick presented a real threat to the public. He looked like a legitimate medical professional, complete with a medical degree, fancy offices, and a thriving practice. Desnick's imprimatur of authority might convince even sophisticated consumers that they needed what were in fact unnecessary surgeries. Dietemann was an entirely different matter. Only a fool would believe in the healing power of Dietemann's quackery. And society's interest in protecting the public from open and notorious charlatans was minimal compared to its interest in encouraging uninhibited conversations.

As a pragmatic defense of the divergent results, this analysis makes sense, but notice the subtext. If the difference between liability and dismissal in an intrusion case is the extent to which the public benefits from the fruits of the intrusion, then non-newsworthiness or something like it has crept into the intrusion upon seclusion tort as a phantom element. There is no place in Prosser's black letter intrusion upon seclusion law to consider the social interest in rooting out charlatans. Yet that seems to be precisely what has occurred in *Desnick v. ABC*, and it suggests the willingness of Judge Posner to lend his voice to the project of reunifying information privacy law.

In the pages that follow, I will briefly sketch out some of the areas in which different branches of the law of privacy have diverged. Many of these divergences have gone unnoticed or unexplained by the courts involved in creating them. I will suggest that the arguments for these divergences are quite weak, and that (among the available models) privacy tort law is probably the most sensible framework for dealing with privacy harms.

II.
THE CONSTITUTIONAL RIGHT TO INFORMATION PRIVACY

In *Whalen v. Roe*,[26] the Supreme Court assumed for the sake of argument that the U.S. Constitution protected individuals against the improper collection, aggregation, or disclosure of their private information. It then held that, even

23. *See* Josh Tyrangiel, *Radiohead Says: Pay What You Want*, TIME, Oct. 1, 2007, http://www.time.com/time/arts/article/0,8599,1666973,00.html.

24. *See, e.g.*, Amy Roe, *A Kirkland Café with No Prices*, SEATTLE TIMES, Feb. 6, 2007, http://seattletimes.nwsource.com/html/businesstechnology/2003558690_terrabite06e.html.

25. *Desnick*, 44 F.3d at 1351–52.

26. 429 U.S. 589 (1977).

under such an assumption, a New York program to track and analyze the prescription of controlled substances did not violate the rights of patients whose doctors prescribed them such medication. Shortly thereafter, the Court again nodded in the direction of constitutional rights to information privacy, but ruled that the public's interest in accessing President Nixon's presidential papers outweighed whatever rights President Nixon may have had in his familial communications.[27] The Court then lost interest in the constitutional right to information privacy for three decades. As a result, *Whalen* and *Nixon* have remained the only two cases in which the Court discussed the constitutional right to information privacy in any detail, though that is about to change this Term, as we shall see in Part VII. In neither case did the party asserting the privacy right prevail.

Constitutional right to information privacy doctrine has been developed significantly in the federal courts of appeals. Most of the appellate courts assume that the Supreme Court intended to recognize a constitutional right of information privacy in *Whalen* and *Nixon*, and have developed frameworks for determining when that right has been violated. By contrast, the D.C. and Sixth Circuits have questioned whether a constitutional right of information privacy exists, given the poorly developed nature of the Supreme Court's jurisprudence.[28] Among the circuit courts that have recognized such a constitutional right, the Third Circuit has worked out its case law most fully.

The leading Third Circuit case that establishes a framework for determining when the constitutional right of information privacy has been violated is *United States v. Westinghouse Electric Corp.*[29] The *Westinghouse* test looks at seven factors to determine whether such a right has been violated: (1) the type of record requested, (2) the information it contains, (3) the potential for harm resulting from nonconsensual disclosure, (4) the injury that disclosure might cause to the relationship in which the information was recorded, (5) the adequacy of safeguards to prevent unauthorized disclosure, (6) the degree of need for access to the information, and (7) whether there is an express statutory command, public policy, or other interest favoring access to the information.[30] Suffice it to say that a test with seven factors and no clear instruction about how to weigh them leads to unpredictable results and is susceptible to significant manipulation.

Where the government improperly collects or publishes a private citizen's personal information, a question arises as to the proper cause of action. In some jurisdictions, sovereign immunity prohibits an individual from suing the state

27. Nixon v. Adm'r of Gen. Servs., 433 U.S. 425 (1977).

28. *See* Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786 (D.C. Cir. 1997); J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981).

29. 638 F.2d 570 (3d Cir. 1980). *Westinghouse* has been cited more than one thousand times as of 2010.

30. *Id.* at 578.

for invasion of privacy.[31] In other jurisdictions, sovereign immunity imposes no such bar because it has been waived via the state's applicable tort claims act.[32] Federal cases typically construe the Federal Tort Claims Act as having waived sovereign immunity in invasion of privacy tort suits against the federal government,[33] though important exceptions apply where federal employees are simply exercising due care to carry out federal policies. Moreover, several states have enacted their own versions of the Federal Privacy Act, which may provide an alternative basis for recovery.[34] Thus, the answer to the question of whether an individual may sue his government for tortious invasion of privacy depends on where he lives, which level of government he is suing, and who within that government has engaged in the wrongful conduct.

The case law thus creates a strange set of circumstances. Suppose that a government employee living in Ohio has his HIV status improperly disclosed by his supervisor to all of his coworkers in contravention of government policy—a fact pattern that has given rise to much litigation. Ohio permits suit for intentional or negligent invasions of privacy.[35] Because Ohio is in the Sixth Circuit, he cannot sue for a violation of his constitutional right to information privacy. If he works for the federal government, he can sue for tortious invasion of privacy. If he works for the state government, Ohio law gets quite complicated.[36] Now transport that plaintiff to Washington D.C. He can certainly sue his (federal) governmental employer under the Federal Tort Claims Act—there is controlling D.C. Circuit authority on point.[37] But he probably cannot sue the same employer under the constitutional right to information privacy—again, there is a D.C. Circuit opinion on point.[38] If the plaintiff lives in Nebraska, he can sue everybody under either a constitutional theory or a tort cause of action—a state governmental employer is liable for either a tort or constitutional violation, as is a federal governmental employer.[39]

---

31. *See, e.g.*, Toomer v. Garrett, 574 S.E.2d 76, 91 (N.C. Ct. App. 2002); University of Texas Medical Branch at Galveston v. Hohman, 6 S.W.3d 767, 777 (Tex. App. 1999); Smith v. City of Artesia, 772 P.2d 373, 374 n.2 (N.M. Ct. App. 1989).

32. *See, e.g.*, Wadman v. State, 510 N.W.2d 426, 429–30 (Neb. Ct. App. 1993).

33. *See, e.g.*, Raz v. United States, 343 F.3d 945, 948 (8th Cir. 2003); Nurse v. United States, 226 F.3d 996, 1002–03 (9th Cir. 2000); Black v. Sheraton Corp., 564 F.2d 531, 540–41 (D.C. Cir. 1977).

34. *See infra* note 73.

35. *See supra* note 12.

36. There is no sovereign immunity for invasion of privacy suits when the act complained of arises out of an employment relationship, though this rule may not apply to intentional invasions of privacy. *See* Nungester v. Cincinnati, 654 N.E.2d 423, 427 (Ohio Ct. App. 1995). There is also the added complication of the Ohio Privacy Act, which seems to waive sovereign immunity for invasion of privacy claims brought under a state statute but not under the common law. OHIO REV. CODE § 1347.10 (2009)

37. *Black*, 564 F.2d at 531.

38. Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791–93 (D.C. Cir. 1997).

39. *See, e.g.*, Alexander v. Peffer, 993 F.2d 1348 (8th Cir. 1993) (recognizing the constitutional right to information privacy, but finding that disclosure by the City of Omaha Police

The courts, by and large, have not devoted attention to the relationship between the constitutional right of information privacy and the invasion of privacy torts.[40] Where the government is the defendant, the harm to the plaintiff is the same regardless of the theory being pursued. Yet, the *Westinghouse* court never explained why it was formulating a doctrine that deviates sharply from privacy tort law. Perhaps the unstated rationale was something along the lines of, "if four elements in a cause of action are good, seven must be even better." But more is not better.

Consider a case like *Doe v. SEPTA*.[41] According to the facts alleged in the complaint, the plaintiff's immediate supervisor improperly discovered Doe's HIV-positive status by obtaining the prescription medication information for each employee under the employer's health plan and quizzing the employer's medical director about what medications were prescribed for which illnesses.[42] The complaint further alleged that the plaintiff's coworkers shunned him socially after the disclosure, though he remained employed. Applying Prosser's public disclosure of private facts framework, the employer's conduct is almost certainly actionable. Doe's HIV status was previously known only to medical personnel at his place of employment, who were on a need-to-know basis. The information was publicized at his workplace, resulting in his social marginalization. The disclosure to coworkers was not newsworthy, because they had no reason to know about his HIV status and he was a low-level employee. And such disclosure was almost certainly highly offensive to a reasonable person.[43] All the elements of a tort would be satisfied. Nevertheless, the court denied a constitutional recovery, holding that under the *Westinghouse* test, the state's interest in controlling the costs of employee medical benefits outweighed Doe's privacy interest. But the harm Doe was alleging had to do with the disclosure of his HIV information to people who would be in no position to make decisions about the employer's medical benefit coverage. Applying a more complicated test, with more factors and more flexibility, distracted the court from the essential issues raised by the plaintiff's complaint.

There have been some decisions that attempt to import tort law principles into the doctrinal framework for the constitutional right to information privacy.[44] The counterpart to Judge Posner's reunifying opinion in *Desnick* is

---

Department of her unsuccessful application to become a police officer was not a constitutional violation because it was not private information).

40. The Washington Supreme Court has held that, where cognizable common law invasion of privacy claims and constitutional privacy claims are asserted simultaneously against a governmental defendant for the same conduct, the court should resolve the common law claims first and decline to reach the constitutional question if the plaintiff prevails under a common law theory. Reid v. Pierce County, 961 P.2d 333, 342–43 & n.6 (Wash. 1998). A double recovery is presumably impossible.

41. 72 F.3d 1133 (3d Cir. 1995).

42. *Id.* at 1135–36.

43. Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491 (Ga. 1994).

44. *See, e.g.*, Russell v. Gregoire, 124 F.3d 1079, 1094 (9th Cir. 1997) (citing common law

Smith v. City of Artesia, in which the plaintiffs alleged that a local police department had improperly circulated crime scene photographs depicting the nude body of their deceased daughter.[45] The court began its analysis with language that seems straightforward, but that subverts existing doctrine: "A review of the scope of the common law right to privacy, although not determinative of the constitutional right, can inform our understanding of the concept of privacy and thereby assist us in evaluating plaintiffs' constitutional claim."[46] The court then reviewed common law precedents holding that the deceased have no privacy rights, as well as constitutional rulings inconsistent with the idea that someone could have a privacy interest in another individual.[47] But by beginning with existing tort law doctrines, the law biased its opinions toward uniformity, not fragmentation.

As with *Desnick*, however, important questions remain about how reunification should proceed. I will argue in Part VII that privacy cases lack a good theory of why constitutional law should supplement tort law as a remedy for government intrusions and disclosures of personal information. An alternative to having constitutional law reflect tort principles would reunify privacy law by doing away with constitutional information privacy law.

Fascinatingly, Freedom of Information Act (FOIA) jurisprudence,[48] like the constitutional right to information privacy case law, provides important examples of judicial efforts to reunify information privacy law. The Supreme Court in *National Archives and Records Administration v. Favish* looked to some common law precedents to determine whether Vince Foster's relatives had a privacy interest in his autopsy photographs under FOIA's privacy exemptions.[49] The Court's unanimous opinion, to which we shall return momentarily, cited four state court opinions granting next of kin privacy rights in pictures of a loved one's corpse—including at least one case that cited *City of Artesia* and other state court decisions finding no privacy rights under these circumstances.[50] Yet the Supreme Court made no reference to any of the contrary authority, no doubt leaving many readers with a false impression that the state law precedents were uniform in recognizing a cause of action for next of kin. Space constraints do not explain the omission because, for good measure, the Court added in a discussion of familial burial rights in *Antigone*.[51]

---

tort precedents to inform the analysis of whether the publication of an ex-offender's residential address and employer under Megan's Law violates the constitutional right to information privacy).

45. Smith v. City of Artesia, 772 P.2d 373 (N.M. Ct. App. 1989).

46. *Id.* at 374.

47. *Id.* at 374–75.

48. 5 U.S.C. § 552 (2006).

49. Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157 (2004).

50. *Id.* at 169 (citing Reid v. Pierce County, 961 P.2d 333, 340–41 (Wash. 1998); McCambridge v. Little Rock, 766 S.W.2d 909, 915 (Ark. 1989); and Bazemore v. Savannah Hospital, 155 S.E. 194 (Ga. 1930)).

51. *See id.* at 168.

We might admire the *Favish* Court's willingness to look to common law precedents (and literature) for guidance while being disappointed at its convenient selectivity in recognizing a privacy cause of action.

III.
FOIA JURISPRUDENCE AND REUNIFICATION

We will stay with FOIA as we explore further instances of privacy law's fragmentation. FOIA was enacted not long after Prosser penned his article. The legislative history concerning its privacy provisions was sparse. Critically, the legislative history is almost entirely silent as to the meaning of the statutory language in exemption 6 (permitting the withholding of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy")[52] and exemption 7(C) (permitting the withholding of "records . . . compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy").[53]

What does this similar language in the two provisions mean? It is natural to analogize between the common law invasion of privacy and the statutory "unwarranted invasion of personal privacy." If the disclosure of information would constitute a tortious invasion of privacy had a private party engaged in it, then the disclosure of the same information by the government would be inappropriate under FOIA. Many state courts have construed the privacy exemptions in their own states' versions of FOIA in precisely that way.[54] But writing in the *Journal of Legal Studies* not long after FOIA's enactment, Tony Kronman wrote that there is nothing in the legislative history of FOIA to suggest that, in adopting this language about unwarranted invasions of personal privacy, Congress meant to import common law tort principles into the law governing FOIA privacy.[55] Although it did not cite this specific language in Kronman's article, the Supreme Court in *U.S. Department of Justice v. Reporters Committee for Freedom of Press* cited other portions of Kronman's article favorably and held that the question whether a disclosure was an

52. 5 U.S.C. § 552(b)(6).

53. 5 U.S.C. § 552(b)(7)(C).

54. *See, e.g.*, Perkins v. Freedom of Info. Comm'n, 635 A.2d 783, 788–91 (Conn. 1993); Jordan v. Motor Vehicles Div., 781 P.2d 1203 (Or. 1989); State Emps. Assn. v. Dept. of Mgmt. & Budget, 404 N.W.2d 606 (Mich. 1987); Child Prot. Grp. v. Cline, 350 S.E.2d 541 (W. Va. 1986); Harris v. Cox Enters., 348 S.E.2d 448 (Ga. 1986); Webb v. Shreveport, 371 So. 2d 316 (La. Ct. App. 1979); Hearst Corp. v. Hoppe, 580 P.2d 246, 252–54 (Wash. 1978); Indus. Found. v. Texas Accident Bd., 540 S.W.2d 668 (Tex. 1976).

55. Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 9 J. LEGAL STUD. 727, 738 n.40 (1980) ("Although the interests protected by FOIA's sixth exemption are similar in many respects to those protected by privacy tort law, neither the legislative history of the act nor its judicial interpretation reveals any reliance on (or familiarity with) the doctrinal contours of the privacy tort . . . .").

invasion of personal privacy under FOIA's exemption 6 was not the same as the question of whether the disclosure would be a tortious invasion of privacy.[56]

Kronman's language has been misinterpreted to imply that FOIA privacy and tort privacy should diverge. It is true that there is nothing in the legislative history to suggest that FOIA privacy should track tort privacy. But it is also true that there is nothing in the legislative history to suggest that FOIA privacy should *not* track the common law. The pertinent question, then, is whether there is any principled basis for thinking that Congress wanted the courts to make up a body of FOIA privacy law that would be inconsistent with privacy tort law.

It is difficult to provide a satisfying explanation for the divergence. It may well be that the law thinks about private speech and government speech differently. From an individual liberty perspective, constraining a private actor from speaking entails an infringement of First Amendment freedoms, but there is no constitutional problem with the federal government constraining its own speech.[57] That dynamic suggests that we might view FOIA privacy and tort privacy differently, perhaps removing non-newsworthiness as a consideration in FOIA privacy disputes.[58] But notice that from the perspective of the data privacy subject, it does not matter whether the government or a private actor is initially disseminating the damaging private information. The FOIA requester often wants to publish the information that the government turns over to him, so the reputational and psychological harm from the disclosure will be equivalent. From an Alexander Meiklejohnian perspective, keeping pertinent information about public affairs out of the hands of the public is equally problematic, regardless of the information's source. Within that framework, one should view public disclosure by the government in response to a FOIA request and public disclosure by a private party in the same terms.

Another plausible basis for distinguishing between FOIA privacy and tort privacy focuses on ex ante information gathering rather than ex post information dissemination. It may be the case that people are only comfortable with turning information over to the government if there are strong privacy protections built into FOIA.[59] In the absence of such a regime, the government could be starved of data about individuals, which would compromise the state's ability to, for example, run effective criminal justice, education, traffic safety, or health care systems. On the other hand, one can make similar arguments

56. U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762 n.13, 772 n.20 (1989). The Court did not cite Kronman's footnote 40 or any other authority for the proposition that FOIA privacy law could deviate from privacy tort law.

57. There is, of course, a body of constitutional law compelling citizen access to government information. *See generally* Adam M. Samaha, *Government Secrets, Constitutional Law, and Platforms for Judicial Intervention*, 53 UCLA L. REV. 909 (2006).

58. More generally, we might say that certain normative frameworks will be hostile to some aspects of the reunification project.

59. A robust Privacy Act may be part and parcel of the same concern.

about the importance of enabling people to trust private actors—be they friends, coworkers, lovers, or private firms that perform essential functions like helping people find information, insuring them against medical costs, disseminating entertainment content to them, or educating them. In short, while ex ante arguments about facilitating information disclosure to government provide a plausible explanation for treating tort privacy and FOIA privacy differently, one would want to construct a difficult empirical and normative argument to support such a distinction. To date, neither courts nor commentators have made such a case.

A more serious objection to treating tort and FOIA privacy similarly builds on FOIA's nature as a mandatory disclosure regime—if none of the FOIA exceptions apply, then a requested document must be disclosed. But the government has unique powers to collect information, thanks to its ability to subpoena documents, conduct wiretaps, access taxpayer information, and so on. The private sector lacks these powers, and the information it possesses therefore might not pose the same level of threat to individuals. This argument has force, but it is counterbalanced by several factors, including the private sector's greater facility with data analysis thanks to reduced agency problems, and Americans' greater willingness to disclose personal information to private entities than to the state.[60] Much of the information in the government's hands is information that high-level policy makers do not realize exists, that is poorly organized, and that may even be difficult to locate. In the private sector, where knowledge is money and money is everything, the incentives to analyze the data that a firm does possess in ways that add value to the firm's bottom line are much more pronounced.[61]

To be sure, the private sector in the United States is not bound by any equivalent of FOIA. If you ask Goldman Sachs to provide you with information about its operations, it can say no to your request—or ignore you completely—without having to provide a privacy rationale or any other justification. But that contrast with FOIA reflects a feature, not a bug. The Freedom of Information Act is a mandatory disclosure regime precisely because Congress was concerned that, in its absence, too much information pertinent to the conduct of government was being kept from the citizenry. To suggest that the FOIA privacy standard ought to be substantially stricter than the tort privacy statute is to privilege one of FOIA's subsidiary purposes (protecting privacy) at the expense of its overarching purpose (promoting disclosure of information

60. In Europe, the private sector is regarded as the much more significant threat to personal privacy, and Europeans may be much more comfortable sharing information with the state than they would be sharing the same information with Google or Microsoft. *See generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

61. The public sector institutions that most closely resemble the private sector—the law enforcement and national security apparatuses—are the ones that can most easily resist FOIA disclosure requests under the statute.

pertinent to the operations of government).

The problematic decision to deviate from privacy tort principles in articulating FOIA privacy law likely has been outcome-determinative in both of the Supreme Court's principle FOIA privacy precedents. In *Reporters Committee*, the Court held that CBS could not use a FOIA request to obtain rap sheet information about a defense contractor who had engaged in dealings with a corrupt congressman.[62] Under privacy tort law, a private party's publication of a story disclosing the contents of a rap sheet that had fallen into private hands would have been lawful. The publication of such information would have informed the public about a matter of great public concern—corruption in Congress and in Department of Defense procurement. As a result of the Court's ruling in *Reporters Committee*, CBS news was given a choice between abandoning an extremely newsworthy investigative story and expending very substantial reporter resources to try to reverse engineer the contents of a rap sheet. Imposing such a burden on the press chills legitimate and valuable news reporting in much the same way as defamation liability. But there is no FOIA equivalent to *New York Times Co. v. Sullivan*.[63] By rejecting privacy tort law's principles, *Reporters Committee* arrives at a result quite hostile to free speech interests. The outcome surely would have distressed Warren and Brandeis.[64]

Similarly, the result in *Favish* probably would have been different under privacy tort principles. In *Favish*, the Court held that FOIA's privacy exemptions justified the withholding of photos taken of Vince Foster's body as it lay in a public park following Foster's suicide.[65] As stated earlier, the tort case law is split with respect to next of kin's privacy interests in autopsy photographs and their ability to recover for public disclosure of private facts. But in none of the pre-*Favish* common law cases that found tort liability did the decedents die in a public place. Their bodies were photographed in private residences, medical examiner's offices, and hospital operating rooms.[66] As a general matter, the privacy tort case law is hostile to the notion that someone badly injured in public has a privacy interest in visual depictions of their

62. U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 780 (1989).

63. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (holding that actual malice is required for public officials to prevail in libel suits).

64. *See* Warren & Brandeis, *supra* note 6, at 214–15.

65. Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 157 (2004).

66. *See* cases cited *supra* note 50. A very recent case, *Catsouras v. Dep't of Cal. Highway Patrol*, 104 Cal. Rptr. 3d 352 (Cal. Ct. App. 2010), does recognize a tort action by next of kin for the dissemination of images of a decedent taken after the car accident that killed her. The accident evidently occurred on a public street. The court relied heavily on *Favish* in sustaining the cause of action, which is a sensible way to try to reunify privacy law. *See id.* at 870–72. The intermediate appellate court should be faulted, however, for failing to consider the competing argument that, under the California Supreme Court's opinion in *Shulman*, the public place where the accident occurred may have eliminated the victim's expectations of privacy.

injuries.[67] In the case of a suicide victim who chose to kill himself in a public place, that resistance would have to be stronger still. Moreover, while the Supreme Court held that the interest in releasing the Foster autopsy photographs was not particularly high, given the similar conclusions to multiple independent inquiries into his suicide, such photographs likely would still count as newsworthy under Prosserian tort law's binary framework.

Even taken on its own terms, the *Favish* Court's conclusion that the autopsy photographs were made less newsworthy as a result of the previous investigations is unsatisfying. Favish requested the photographs because he believed that there was a conspiracy to cover up Foster's murder, and the Court noted that multiple separate investigations had debunked that murder theory. But suppose Favish had sought the release of the photographs to suggest different wrongdoing by the government—not its murder of a high government official, but its wasteful expenditure of resources on multiple investigations of what was obviously an open-and-shut case of suicide. Under the reasoning of the *Favish* opinion, a person seeking the disclosure of the autopsy photographs under such a theory ought to be able to prevail under the Court's balancing approach. If we take the reasoning of the opinion seriously, you or I should be able to obtain the Foster autopsy photos if we just recharacterize the government's misconduct.

In short, the Supreme Court has made errors in both of its landmark FOIA privacy precedents and those are mistakes that would have been averted had FOIA privacy doctrine simply followed well-established privacy tort principles. The incoherence of privacy law is not just a problem for those who would like to see conceptual clarity in the law. It also results in outcomes that impede significant speech interests as well.

IV.
DISCLOSURE UNDER THE PRIVACY ACT

The federal Privacy Act[68] is in some ways the most ambitious piece of federal legislation in the domain of information privacy. It is certainly the most comprehensive law that regulates the processing and dissemination of information that the government collects about individuals.[69] The two events precipitating the enactment of the Privacy Act in 1974 were the abuses of the Watergate era, in which the Nixon administration used the federal government's access to personal information to identify and intimidate its political opponents, and the development of the Fair Information Practices, a comprehensive framework of privacy principles that were designed to help privacy law meet the new challenges posed by computerization.

---

67. Shulman v. Group W Prods., Inc., 955 P.2d 469, 490 (Cal. 1998).

68. 5 U.S.C. § 552(a) (2006).

69. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 583 (1995).

The key language in the Privacy Act prohibits agencies of the federal government from disclosing "any record which is contained in a system of records . . . to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[70] The law defines "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history."[71] The legislative history of the Privacy Act focuses heavily on the imperative that the government prevent the disclosure of "personal information," and some courts have concluded that only "personal information" can constitute a "record" under the Privacy Act.[72] But whereas state versions of the Privacy Act, like the legislative history of the federal Privacy Act, refer to "personal information" associated with data privacy subjects, the federal legislation's text refers simply to "records."[73] Some federal courts have taken this word choice to mean that the law protects individuals against governmental disclosure of information that is *by no means private*, the title of the statute notwithstanding.

The leading on-point case is *Quinn v. Stone*.[74] That case involved two individuals who went hunting on property belonging to an Army depot where both were employed.[75] This hunting was permitted, as long as the hunters first provided their hunting license numbers, names, addresses, phone numbers, and permit numbers when signing into a hunting registry. After signing in and beginning their hunt, the plaintiffs came under suspicion of illegally evading regulations concerning the number of deer that could be killed in a season. A wildlife conservation officer was contacted to investigate whether any illegal conduct had occurred. In the course of his investigation, the officer examined the hunting registry and also obtained one of the plaintiff's time cards to investigate a (false) allegation that she had been hunting on a day when her employer thought she was at work.[76] The officer's investigation eventually concluded that the plaintiffs' conduct had been lawful, and the investigation was closed. The plaintiffs then sued the Secretary of the Army for violating the Privacy Act by disclosing the information on the hunting registry to the conservation officer.

---

70. 5 U.S.C. § 552a(b).

71. 5 U.S.C. § 552a(a)(4).

72. Houston v. U.S. Dep't of Treasury, 494 F.Supp. 24, 27–28 (D.D.C. 1979).

73. For a nice comparison of federal and state language, see *Privacy Acts of the States and the United States*, TEXAS ATTORNEY GENERAL, http://www.oag.state.tx.us/notice/privacy_table.htm (last visited March 22, 2010).

74. Quinn v. Stone, 978 F.2d 126 (3d Cir. 1993).

75. *Id.* at 128–29.

76. *Id.* at 130.

One of the defendant's principal claims was that it could not be liable for disclosing to an investigator information—an address and telephone number here—that was "readily accessible to the public."[77] One of the plaintiffs had listed his address and phone number in the local telephone directory. Remarkably, the court held that while there could be no liability under the Privacy Act if the investigator already knew the plaintiff's phone number and address, liability was appropriate if the information was merely "readily accessible to the public."[78] The court wrote:

> Appellees have cited to this court no case that stands for the proposition that there is no violation of the Act if the information is merely readily accessible to the members of the public (such as in the local telephone book) and our research has discovered none. We doubt if any court would so hold. To do so would eviscerate the Act's central prohibition, the prohibition against disclosure. . . . To define disclosure so narrowly as to exclude information that is readily accessible to the public would render superfluous the detailed statutory schemes of twelve exceptions to the prohibition on disclosure. We conclude that making available information which is readily accessible to members of the public is a disclosure under [the Act] . . . .[79]

In short, the court said, the temporal sequence of the disclosure matters a great deal. If, upon learning information that might cause him to believe that the plaintiff may have behaved unlawfully, the investigator had looked up the plaintiff's address in the phone book, there would be no Privacy Act violation as a result of the Army's subsequent disclosure of the address to the investigator. But the Army's disclosure violated the Act because it happened before the investigator had done this rudimentary detective work.

Such reasoning is difficult to square with the law's general attitude toward harm and causation. One way of understanding information "readily accessible to the public," is to define such information as information whose disclosure is inevitable to interested parties. By being placed on notice that the plaintiffs may have broken the law, the wildlife conservation officer almost certainly would have had reason to obtain the telephone number and address of the investigation's targets so that he could seek to question them about their conduct. In public disclosure tort law specifically, and tort law in general, the core inquiry is whether, in the absence of the defendant's actions, the information at issue would have remained private.[80]

There is no good theory for why the Privacy Act should either compensate plaintiffs or punish the government for the disclosure of information that is

77. *Id.* at 134.

78. *Id.*

79. *Id.* at 134 (footnote omitted).

80. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 935 (2005).

already readily accessible to the public. One wants to deter the government from disclosing information where such disclosure is harmful to individuals, but not to deter a government disclosure that harms no one. While there may be a case for implementing the FOIA standard from *Reporters Committee*—the government should not be permitted to disclose "practically obscure" information about an individual—the case against such disclosure collapses when the information at issue is not even practically obscure.

The rule in *Quinn v. Stone* simply engenders absurd results. The Army must pay damages for the disclosure to an investigator of the address and telephone number of a person of interest in a criminal investigation. In *Pilon v. United States Department of Justice*,[81] the D.C. Circuit held that the government could be liable under the Privacy Act for disclosing information to an individual that the individual already knew based on his previous employment experience with the agency that had released the information. The court arrived at this conclusion after devoting seven pages to the interpretive question of whether the government "discloses" information to an individual when it releases to that individual information he already knows.[82] The court noted that dictionary definitions for "disclose" sometimes encompass the dissemination of information to people already in possession of it, provided a smattering of fairly weak examples, and observed that in several places the statute seems to refer to disclosure and dissemination interchangeably.[83] But while considering the plain meaning and legislative purpose of the Privacy Act, the court never once thought to consider the title of the statute. Under no version of privacy law—save the Privacy Act after *Quinn* and *Pilon*—can information be private with respect to someone who already knows it. As the court acknowledged, the Act emerged from "a late-session congressional compromise, with several of its central terms lacking express definition."[84] It is plausible, likely even, that few in Congress read the bill's provisions. But surely all of them knew the law's name. Yet the *Pilon* court announced itself unwilling to reject even the extraordinary proposition that the disclosure of "a document that has already been fully aired in the public domain through the press or some other means" could violate the Privacy Act.[85]

The result in *Pilon* is not indefensible. A sensible argument for *Pilon* would focus on the ability of the information recipient to disseminate that information to third parties. Thus, a former or present government employee might be barred by ethical or contractual obligations from disclosing information she learned while working for the government, but if she received the duplicative information lawfully from another agent of the government via

81. 73 F.3d 1111 (D.C. Cir. 1996).
82. *Id.* at 1117–24.
83. *Id.*
84. *Id.* at 1112.
85. *Id.* at 1123 n.10.

FOIA, her ability to pass the information on to the press or a third party could be constitutionally protected. Read in this manner, *Pilon* might be part and parcel of the *Reporters Committee* reasoning that information can still be private when it is merely practically obscure. Having said that, it is very hard to construct a persuasive argument for the correctness of both *Pilon* and *Quinn*. Now we are talking about information to which the press and the public already have easy access. The former government employee who wants to share information learned during her employment can do so easily via public documents. The concern about a former employee "laundering" previously private information into public information disappears completely.

To summarize the discussion so far, the federal appellate courts have made a mess of things. Seizing on an open-ended word choice in the legislation while ignoring much of its legislative history, the courts have read the word "privacy" out of the "Privacy Act." The result is an unusual situation in which the federal government may be liable for disclosures that harm no one. This would not be a problem were a plaintiff's recovery limited to actual damages under the statute. The absence of harm would entail the absence of a remedy. But the Privacy Act contains a minimum statutory damages provision, which reads as follows:

> In any suit brought under the provisions of . . . this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of –
>
> (A) Actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000; and
>
> (B) The costs of action together with reasonable attorney fees as determined by the court.[86]

Now we see the potential for difficulties. The government might intentionally release a record containing exclusive information that is already readily accessible to the public. No harm would ensue, but the government would still be liable for $1,000 per violation. In the case of a large-scale disclosure concerning many individuals, the government could face enormous liability.

Enter *Doe v. Chao*, the Supreme Court's most significant decision concerning the Privacy Act.[87] In *Chao* the Court had to construe the law's minimum damages provision. Doe was a worker who applied to the Labor Department for benefits under the Black Lung Benefits Act. His application for benefits asked for his Social Security number, which the Department then used as the reference number for Doe's claim. As a result, the number was sent to groups of other claimants and their lawyers. Doe's number, along with those of

86. 5 U.S.C. § 552a(g)(4)(A) (2006).
87. 540 U.S. 614 (2004).

his fellow plaintiffs, was compromised, subjecting them to a heightened risk of identity theft. Yet, when the case was litigated, Doe had not been victimized by identity thieves. Rather, Doe asserted that he was "greatly concerned and worried" about the improper disclosure of his Social Security number.[88] He did not corroborate this testimony with evidence of medical treatment, out-of-pocket expenditures to remedy the situation, or other documented loss of income.

In a 6-3 decision, the Court held that Doe was not entitled to the $1,000 statutory minimum. The Court read subsection (a) of the statute to entitle only someone who had sustained "actual damages" to recover the $1,000 minimum.[89] Along the way, the Court held that subsection (a)'s reference to a "person entitled to recovery" meant someone who had sustained "actual damages."[90] The clear implication of the Court's analysis is that if Doe had spent, say, $20 for a credit-monitoring identity theft program, he would be entitled to at least $1000 in damages, but because he could not demonstrate such expenditures he was entitled to nothing. That seems odd. Two very interesting passages from Justice Souter's majority opinion try to parry this concern:

> Doe's manner of reading "entitle[ment] to recovery" as satisfied by adverse effect caused by intentional or willful violation . . . is at odds with the traditional understanding that tort recovery requires not only wrongful act plus causation reaching to the plaintiff, but proof of some harm for which damages can reasonably be assessed.
>
> . . . .
>
> Doe also suggests there is something peculiar in offering some guaranteed damages, as a form of presumed damages not requiring proof of amount, only to those plaintiffs who can demonstrate actual damages. But this approach parallels another remedial scheme that the drafters of the Privacy Act would probably have known about. At common law, certain defamation torts were redressed by general damages but only when a plaintiff first proved some "special harm," *i.e.*, "harm of a material and generally of a pecuniary nature." . . . Because the recovery of presumed damages in these cases was supplemental to compensation for specific harm, it was hardly unprecedented for Congress to make a guaranteed minimum contingent upon some showing of actual damages, thereby avoiding giveaways to plaintiffs with nothing more than "abstract injuries."[91]

Fascinating stuff. The Court is telling us that tort principles will aid interpretation of the Privacy Act's ambiguous minimum statutory damages language. Yes, the hypothetical Doe who signs up for identity theft protection

88. *Id.* at 618.
89. *Id.* at 616.
90. *Id.* at 620.
91. *Id.* at 621, 625–26 (citations omitted).

with Equifax would be treated differently than the real Doe, but the same would be true under ordinary tort principles of recovery. As with FOIA, there is nothing in the Privacy Act to say whether tort law conceptions influenced the legislators who voted for the bill, but the majority finds the arguments for coherence attractive nevertheless. Read together, *Chao* and *Favish* stand for a kind of "coherence canon," whereby statutes are interpreted by the courts so as to minimize any conflicts with common law developments in closely related subject matters.

Justice Ginsburg's dissent in *Chao* makes several compelling statutory interpretation arguments. As she pointed out, the majority's construction of the language renders the statute's "adverse effect" element for liability superfluous, and it converts the law's "shall be liable" into "may be liable."[92] The dissent is quite effective in explaining that similar language in other federal statutes had been construed to permit recovery of minimum damages without a showing of pecuniary harm.[93] There were, moreover, strong arguments that the dissent did not raise too. Notice, for example, that Congress used "but" in between the clause entitling plaintiffs to "actual damages" and the clause setting a $1,000 floor for recoveries.[94] If the majority is right about what Congress meant then "and," rather than "but," seems the appropriate conjunction. For these reasons, I was one of sixteen privacy law scholars who signed an amicus brief urging the Court to rule in Doe's favor.[95] No academics doing work in the area submitted amicus briefs in support of the Labor Department's interpretation. The majority's statutory interpretation arguments are not demonstrably wrong, but when the respective opinions are placed side by side it is very surprising that Justice Souter's is the one that garnered more votes.

I still think the Court got it wrong in *Doe v. Chao*, but I now believe I understand what the majority may have been attempting to do. We can understand *Chao* as another exemplary "reunifying privacy law" opinion—akin to *Desnick* or *City of Artesia*. Faced with the prospect of crippling liability for government disclosures of information that was already readily accessible to the public, the Court fixed the problem in a "second best" way. Rather than overruling *Quinn* directly, the Court took the wind out of its sails. Where information is already readily accessible to the public, the person whom that information concerns cannot show harm from the government disclosure. And absent a showing of harm, there is no incentive to bring a suit. *Chao*, in short, is the second wrong that made a right.

---

92. *Id.* at 631 (Ginsburg, J., dissenting).

93. *Id.* at 639–41.

94. *See supra* text accompanying note 86.

95. *See* Brief for Electronic Privacy Information Center et al. as Amici Curiae Supporting Petitioner, Doe v. Chao 540 U.S. 614 (2004) (No. 02-1377), 2003 WL 22070504. That was the only amicus brief the author has ever signed, and the author has now learned his lesson.

So far, *Chao* has had little impact on the *Quinn-Pilon* line of doctrine. Recent cases continue to cite those precedents as good law as if nothing has changed.[96] But things have changed, and dramatically. The Supreme Court has told us that tort principles concerning harm and damages comprise an essential part of the appropriate judicial methodology for interpreting the Privacy Act. So if principles from a pocket of tort law like defamation may prove decisive in helping judges decipher the meaning of ambiguous terms, principles from privacy tort law must be all the more germane. Yet *Quinn* and *Pilon* are not just out of step with privacy tort principles—they are in a completely different galaxy.[97] Properly understood, *Chao* points toward the radical revision of Privacy Act jurisprudence. But almost no one has noticed.

There is a recent and encouraging exception. In June, the D.C. Circuit handed down *Armstrong v. Geithner*,[98] a Privacy Act case that used tort principles—and even privacy tort scholarship—to decide whether the Privacy Act protected an individual who was seeking to transfer from one part of the federal bureaucracy to another. Someone with knowledge of an ongoing investigation of Armstrong by the Treasury Inspector General for Tax Administration (TIGTA) (his old employer) informed six employees at the United States Department of Agriculture (USDA) (his new employer) that TIGTA was investigating Armstrong for misconduct. After learning of the probe, the USDA postponed Armstrong's start date indefinitely.[99]

Armstrong could not prove that the anonymous person who leaked the information to the USDA had retrieved the information from a "system of records," but he offered the court a tort-based *res ipsa loquitur* argument, suggesting that the information could only have come from a source of information protected by the statute.[100] Writing for the court, Judge Ginsburg applied tort-style causation analysis to determine whether the Privacy Act had been violated, concluding that no violation had occurred.[101]

For good measure, the court then added an alternative basis for dismissing Armstrong's suit. It noted that Armstrong himself had disclosed aspects of the investigation to eight people—his wife, five coworkers, and two people outside

96. *See, e.g.*, Scarborough v. Harvey, 493 F. Supp.2d 1, 16 n.29 (D.D.C. 2007).

97. There must be some logical stopping point to this argument, where tort law ceases to shape Privacy Act interpretation. The clearest example of this is the law's reference to criminal history information as information that plainly constitutes a record, the disclosure of which may violate the Privacy Act. *See supra* text accompanying note 71. Although this was not true at the time the Privacy Act was enacted, it is now well established that the publication of someone's prior criminal history cannot be tortious under American law. *Compare* Briscoe v. Reader's Digest, 483 P.2d 34 (Cal. 1971) (holding that the publication of an eleven-year-old criminal conviction may be tortious), *with* Gates v. Discovery Commc'ns, Inc., 101 P.3d 552 (Cal. 2004) (holding that *Briscoe* must be overruled in light of subsequent U.S. Supreme Court precedents).

98. 608 F.3d 854 (D.C. Cir. 2010).

99. *Id.* at 856.

100. *Id.* at 857.

101. *Id.* at 859.

TIGTA.[102] Citing a law review article that proposes a framework for determining when such disclosures waive a "reasonable expectation of privacy" under privacy tort law, the court concluded that one of these disclosures might well have started the causal chain that resulted in the information's disclosure to TIGTA.[103] Noting that as an empirical matter, disclosures of sensational information were likely to spread like wildfire through a workplace, the court concluded that "Armstrong's disclosures to seven professional contacts could easily account for certain details finding their way into the TIGTA rumor mill."[104] Perhaps the radical revision of Privacy Act jurisprudence hinted at in *Chao* is now underway.

V.
A FRAMEWORK FOR REUNIFYING PRIVACY LAW

To say that privacy law should be reunified along the lines described by Warren and Brandeis is not to suggest that in 1890 they gave us everything the law needs to navigate the privacy challenges arising in contemporary society. Nor do I wish to suggest that privacy law should become fixed or, worse, stagnant. The Warren and Brandeis vision of privacy law was one that expressed a strong common law sensibility, and one that was optimistic about the potential for scholarship to lend coherence to the common law's path. In the pages that follow I will sketch out a general vision of what a reunified privacy law framework might look like, and how it might address current controversies in privacy law.

The first step is to thank Prosser for his attention to and insights about privacy law, and the second is to turn our backs on basically everything he sought to accomplish. There is no reason why the torts for intrusion upon seclusion and public disclosure of private facts should look different from each other. The keys to each tort are whether the defendant's actions intruded upon private information and whether the defendant's conduct violated existing norms of social conduct—in other words, whether the conduct was highly offensive to a reasonable person. We should add to this inquiry the basically welfarist balancing test that Warren and Brandeis embraced in 1890 and that Judge Posner snuck back into the law in *Desnick*: Is the gravity of the harm to the plaintiff's privacy interest outweighed by a paramount public policy interest, such as the need to protect patients against quack doctors or the public purse against Medicare fraudsters?

To be sure, two important distinctions remain between intrusion harms and public disclosure harms. First, we may expect that the damage to the plaintiff is greater in cases involving a public disclosure, precisely because

102. *Id.* at 861.
103. *Id.* at 860–61 (citing Strahilevitz, *supra* note 80, at 919).
104. *Id.* at 861.

reputational harms compound dignitary harms, and the reputational harms in a pure intrusion case are necessarily limited. This is a principle that the law already recognizes, and it shows up in lower damage awards for cases involving no publication of the private facts. Indeed, jurisdictions like Illinois and Michigan have practically eliminated "publication" as an element of Prosser's publication of private facts tort by finding liability where the defendant disseminated private information to a small number of individuals who have a "special relationship" with the plaintiff—another reunifying thread in privacy tort law.[105]

The second distinction seems more fundamental but is as neatly resolvable. The First Amendment implications of limiting a defendant's ability to disclose facts are more troublesome than the implications of limiting a defendant's ability to gather facts. Although this distinction is not immune to criticism, let us assume its correctness for the sake of argument. The fact that the First Amendment may constrain the state's ability to impose damages on those who publish private facts does not mean that the underlying tort causes of action need to look any different. Rather, it simply means that once tort liability is found, the courts should conduct an independent inquiry as to whether imposing liability on that defendant (or class of defendants) will undermine fundamental expressive or self-governance interests. Indeed, such a textured inquiry better coheres with First Amendment doctrine than does the public disclosure tort's binary newsworthiness/non-newsworthiness distinction.

By introducing non-newsworthiness as an element of the public disclosure tort, Prosser brought First Amendment interests into the tort, yet this is not obviously where they belong. The tort of intentional infliction of emotional distress sometimes involves hurtful speech that is nevertheless of legitimate concern to the public. This situation has not prompted tort scholars to develop multiple versions of the tort. Rather, courts simply consider the First Amendment implications of imposing liability through a separate inquiry when required to do so.[106]

Returning privacy tort law to the 1890s-era status quo is attractive, and it does not require the replacement of Prosser's framework with element-less torts. We can embrace a reformed version of Warren and Brandeis's unified tort for invasion of privacy. Such an invasion occurs when the defendant infringes upon (1) the defendant's private facts or concerns, (2) in a manner that is highly offensive to a reasonable person, and (3) engages in conduct that engenders social harms that exceed the associated social benefits.

---

105. Beaumont v. Brown, 257 N.W.2d 522 (Mich. 1977); Miller v. Motorola, 560 N.E.2d 900 (Ill. App. Ct. 1990).

106. The Supreme Court has allowed the states to leave intact the elements of a state law intentional infliction of emotional distress cause of action but held separately that the First Amendment requires public figure plaintiffs to demonstrate actual malice in order to recover. *See* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 56 (1988).

Having achieved the perfect fix for all the problems with privacy tort law,[107] we can turn to the privacy statutes. Here too, a privacy tort model seems poised to offer results that are reasonably predictable and efficient. This Article has already shown how the Privacy Act and FOIA might be interpreted through a privacy tort law prism. Overlaying such an approach onto the Electronic Communications Privacy Act (ECPA), the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), and other landmark pieces of privacy legislation makes sense too. Certainly, privacy tort law has been spared the withering criticism to which ECPA's obsolete medium-based privacy hierarchy has been subjected.[108]

The thornier issues arise as we contemplate those privacy harms that are not easily remedied through existing tort law. At first glance a unified privacy tort might have a hard time dealing with issues like data mining, behavioral marketing, telemarketing, social networking websites, or location-aware smartphones. But there have been many opportunities presented for judges to address these problems via tort rules. In some cases that might compromise an individual's safety, such as sales of personal information by data brokers, the courts have been willing to expand tort liability to regulate the dangerous conduct.[109] But in the majority of cases, the courts have understood themselves to be junior partners to legislators and regulators in dealing with new privacy challenges.[110] The possibility that legislators might want to legislate has convinced the courts to stop innovating through common law. And the unwillingness of judges to modernize tort protections to deal with new challenges has prompted legislators in turn to legislate in ad hoc, often incoherent ways.

---

107. I am kidding.

108. For a few examples of ECPA-bashing, see Fredrick M. Joyce & Andrew E. Bigart, *Liberty for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Pervasively Electronic World*, 41 VAL. U. L. REV. 1481, 1495 (2007) ("A random sampling of cases involving alleged violations of the ECPA and other electronic privacy laws reveals a crazy-quilt of fact-specific outcomes. There is no unitary theme to these case precedents; they offer little practical guidance to those who engage in electronic communications and to those who are entrusted to protect electronic communications and records."); Patricia M. Worthy, *The Impact of New and Emerging Telecommunications Technologies: A Call to the Rescue of the Attorney-Client Privilege*, 39 HOW. L.J. 437, 450 (1996) ("The attempt by Congress, through the enactment of ECPA, to recognize and effectuate policy for the new and emerging technologies, served only to create irrational categories of protected communications.") (footnote omitted); President's Working Group on Unlawful Conduct on the Internet, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET III.D.1., http://www.justice.gov/criminal/cybercrime/unlawful.htm (March 2000) ("[A]dvances in telecommunications technology have made the language of the statute obsolete.").

109. Adler v. Vision Lab Telecommc'ns, 393 F. Supp.2d 35, 42 (D.D.C. 2005); Remsburg v. Docusearch, 816 A.2d 1001 (N.H. 2003).

110. *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. Ct. App. 1995); Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975).

In principle, the great privacy innovations of the twentieth century—like the Fair Information Practices—can be incorporated into privacy tort law.[111] Tort law could simply require entities that hold personal information about individuals to: disclose the presence of dossiers to data privacy subjects if asked about them; provide opportunities for data privacy subjects to correct errors in those dossiers when they can show that such information is indeed erroneous; obtain the subject's informed consent when sensitive data is transferred to another entity for another purpose; and take reasonable precautions to safeguard personal data against misuse or theft. To the extent that these obligations exist at all in U.S. law, they are statutory, but there is no reason why they could not be part of the common law.[112] Indeed, common law adjudication might permit the seamless and rapid application of the Fair Information Practices principles to new kinds of privacy threats like Facebook Beacon or Google Buzz.

Of course, it is always possible that Congress will endeavor to reunify privacy law via comprehensive privacy legislation. As Paul Schwartz and Karl-Nikolaus Peifer's wonderful article in this volume makes clear, Germany has embraced a largely coherent vision of privacy law grounded in the right of personality.[113] There is an effort underway in the Australian legislature to enact such legislation, and the pending Australian legislation that would replace that country's existing Privacy Act consciously attempts to create parity between the demands placed on the public sector and those imposed on the private sector.[114] In the last Congress, two pieces of legislation, the Boucher Bill and the Rush Bill, were introduced. Neither was enacted. Both bills were described as comprehensive privacy legislation.[115] While these bills tackled consumer privacy issues that are largely unregulated, it was inaccurate to describe them as comprehensive privacy bills. They attempted to regulate practices concerning data retention, data security, and transfers of privacy legislation.

---

111. For a discussion of the Fair Information Practices, and their applicability to contemporary privacy challenges, see Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

112. Of course, it could well be that some of the harms emphasized by the Fair Information Practices are discrete, collective harms that are suffered by very large numbers of people. Such harms may appear less salient in a tort case, when an individual claimant is seeking relief. Mechanisms for aggregating such dispersed claims, such as class action suits, have well-known flaws.

113. Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIF. L. REV. 1925 (2010).

114. *See* Karin Clark, *Two Senate Enquiries into the Protection of Privacy in Australia*, THE FORTNIGHTLY REVIEW OF IP & MEDIA LAW, http://fortnightlyreview.info/2010/07/15/two-senate-enquiries-into-the-protection-of-privacy-in-australia/ (last visited Aug. 11, 2010); Exposure Draft, *Australian Privacy Principles*, SPECIAL MINISTER OF STATE, http://www.smos.gov.au/media/2010/docs/privacy-reform-exp-draft-part-1.pdf.

115. Richard Raysman & Peter Brown, *Contractual Nature of Online Policies Remain Unsettled*, N.Y.L.J., Aug. 10, 2010.

But numerous privacy issues remained well beyond their scope. These bills would have brought more coherence to some aspects of privacy law, but they made no attempt to engage in anything like the reunification project described in this Article.

There is no principled reason why a future Congress could not attempt to enact truly comprehensive privacy legislation, preempting inconsistent state laws and amending the various existing federal privacy frameworks to achieve coherence. Yet there are a number of pragmatic reasons why such a step is unlikely. Existing legislative frameworks create constituencies that would resist changes that might take away victories hard won in past legislatures. Public choice dynamics push legislatures away from efficient sets of rules and toward systems that reward discrete, well-organized interest groups. Legislators strive for compromises, not analytical elegance. If Schwartz and Peifer's claim that Americans are less inclined than Germans toward theoretical unification and philosophical rigor is right,[116] then the tendency is surely more pronounced in our legislators than our jurists.

VI.
THE DESIRABILITY OF COHERENCE IN PRIVACY LAW

Coherence in privacy law is basically achievable. The question remains whether such coherence is normatively desirable. The answer is yes, for two reasons.

First, coherent law lowers the compliance costs for individuals and organizations. Just as firms doing business in a number of markets typically prefer that the laws of various jurisdictions be harmonized, they will also prefer that the different common law and statutory frameworks governing their conduct direct them to similar ends. A modern firm like Google or Microsoft will have on staff lawyers who deal regularly with ECPA, FACTA, HIPAA, CFAA, CALEA, COPPA, FERPA, CAN-SPAM, and FISA, plus common law torts and European Union privacy directives. Government lawyers may need to familiarize themselves with each of these statutory frameworks, as well as the Privacy Act, FOIA, and the constitutional right of information privacy. Safeguarding privacy interests is most cost effective when the provisions in this alphabet soup do not conflict with one another, and when knowledge about one privacy system can be leveraged to help understand another. When FOIA privacy and Privacy Act privacy mean different things, and FOIA penalizes nondisclosure but the Privacy Act penalizes disclosure, government lawyers necessarily find themselves stuck between a rock and a hard place. Incoherent law is inefficient law. It is expensive law. It is confusing law that may lead even skilled and industrious lawyers astray.

116. Schwartz & Peifer, *supra* note 113.

Second, the complexity and fragmentation of privacy law limits the gains available in common law adjudication. When courts treat Privacy Act law, FOIA privacy, or privacy tort law as a walled garden, they require that wheels be reinvented and they enhance uncertainty among private parties trying to figure out how to conform their behavior to the law's requirements. There are inevitably issues about what counts as private that arise first in FOIA privacy law, but that will ultimately arise in tort, and vice versa. When courts deem the law of FOIA privacy off limits for privacy tort purposes they necessarily impoverish the case law of helpful precedents.

The product of all this is an environment where judges have a relatively free hand to reunify privacy law selectively, quite possibly in a results-oriented way. Take the question of whether an individual has a privacy interest in his residential address. FOIA says that such an interest exists and the government can withhold the addresses of federal workers.[117] Privacy tort law says that the interest does not exist and there is no civil liability for disclosing the home address of an individual.[118] In a Ninth Circuit constitutional right to information privacy case challenging Megan's Law, the court cited only the tort precedents to hold that ex-offenders had no protected privacy interest in their addresses.[119] In a Third Circuit constitutional right to information privacy case challenging Megan's Law, the court cited only the FOIA privacy precedents to hold that ex-offenders possessed a protected privacy interest in their home addresses.[120] Once again, this sort of incoherence goes unrecognized whenever we excuse privacy law's fragmentation.[121]

Nonetheless, incoherence has its benefits. Information privacy law is a complex system, and it is worth thinking through the dangers that might be posed if the law becomes uniform. One is the danger of assuming that all contexts are alike. If people inevitably and correctly regard the disclosure of their private information to the state and civil society very differently, then trying to create coherence between the legal systems governing these disparate threats will be misguided. Alternatively, we might worry that the law is coherent *but wrong*. If mistakes in the Privacy Act are immediately duplicated in privacy tort law or FOIA privacy law, then the damage from the initial mistake will be magnified. These concerns are closely related, and judges are the stopgap in both instances. Courts must be able to recognize when an analogy breaks down, and must continue to do what the common law tradition

117. U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 502 (1994).

118. Johnson v. Sawyer, 47 F.3d 716, 732–33 (5th Cir. 1995) (en banc).

119. Russell v. Gregoire, 124 F.3d 1079, 1094 (9th Cir. 1997).

120. Paul P. v. Verniero, 170 F.3d 396, 403–04 (3d Cir. 1999).

121. It is coherent to conclude that society should give greater respect to federal employees' privacy interests in their home addresses than to sex offenders' privacy interests in their home addresses. But that would result from the greater societal interest in disseminating the information, not the sex offenders' lesser interest in privacy. This is the most charitable reading of *Paul P.*'s holding, which does uphold Megan's Law. *Id.* at 404.

asks of them—scrutinize precedents from peer and inferior courts carefully, follow them when appropriate, and reject them when their premises have been falsified or when their analysis does not persuade.

VII.
CAN *NELSON* FOLLOW *MAYNARD*?

Let us conclude by considering two striking contemporary developments in American privacy law. On August 6, 2010, not long before this Article went to press, the D.C. Circuit, in a *tour de force* opinion by Judge Ginsburg, went farther toward the reunification of information privacy law than any court to date. *United States v. Maynard* raised the question of whether the warrantless twenty-four-hour monitoring of a criminal suspect's travels for four consecutive weeks via GPS amounts to a search under the Fourth Amendment.[122] The court held that such monitoring did violate the defendant's reasonable expectation of privacy, noting that the U.S. Supreme Court had reserved the question whether "dragnet-type" warrantless twenty-four-hour surveillance would violate the Constitution in an earlier case that had authorized the use of beepers to monitor the movements of a suspect's vehicle.[123]

The *Maynard* opinion's embrace of a coherent body of information privacy law was more complete than anything written since Warren and Brandeis's time. The opinion cited *Reporters Committee* for the view that the sum of the whole could be greater than the sum of the parts where threats to privacy were concerned, and *Reporters Committee's* logic is relatively satisfying in contexts like this one that do not implicate free speech interests.[124] Thus, the difference between pervasive twenty-four-hour GPS monitoring over four weeks and short-term GPS monitoring for a few days would be far more than merely a matter of degree. In addition to citing various state and federal Fourth Amendment cases on GPS surveillance, and state statutes requiring the use of a warrant before GPS monitoring can occur,[125] the opinion analyzed at some length precedents from tort law, including landmark tortious intrusion upon seclusion cases like *Galella v. Onassis* and *Nader v. General Motors*.[126] Both those opinions noted the privacy dangers posed by overzealous surveillance in public places that provided the subject with no opportunity to escape by blending in with the crowd. Continuing in that vein, the *Maynard* court emphasized the extent to which twenty-hour extended surveillance could

122. United States v. Maynard, 615 F.3d 544, 555 (D.C. Cir. 2010).

123. *Id.* at 556 (citing United States v. Knotts, 460 U.S. 276 (1983)).

124. *Id.* at 561.

125. *Id.* at 562–65.

126. *Id.* at 562–63 (citing Galella v. Onassis, 353 F. Supp. 196 (S.D.N.Y. 1972) and Nader v. General Motors, 25 N.Y.2d 560 (N.Y. 1970) (Breitel, J., concurring)). While free speech interests are not implicated, public safety interests are, meaning that applying *Reporters Committee* is controversial here too.

reveal sensitive facts about an individual that would not be discernable through fleeting monitoring:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. . . . Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.[127]

This sophisticated analysis is more similar in substance to the sort of thinking that courts have historically done in privacy tort cases than in Fourth Amendment cases. But the *Maynard* court is implicitly asking a very fine question, which is: "why should there be any difference between these bodies of information privacy law?"

The second great innovation in *Maynard*, another that was borrowed from privacy tort law, is the idea that real-world resource constraints color an individual's reasonable expectations of privacy. As I explained in *A Social Networks Theory of Privacy*, tort law typically analyzes expectations of privacy through a probabilistic lens. If it is theoretically possible, but extraordinarily unlikely, that information shared with a few individuals will ultimately become widely known by the public, then privacy tort law usually discounts the theoretical possibility and holds that the data privacy subject maintains a reasonable expectation of privacy.[128]

Some Fourth Amendment cases do the same thing. For example, in *Kyllo v. United States*, the Court held that a homeowner had a reasonable expectation that technologies not in general public use would not be employed by the police to gather information about the interior of a home, but could harbor no such expectation as to technologies that were commonly used by members of the public.[129] And in *Ferguson v. City of Charleston,* the Court held that pregnant women retained a reasonable expectation of privacy in their urine samples that were collected at a state hospital, such that samples that tested positive for cocaine could not be turned over to the police as a matter of course.[130] The Court reached this conclusion even though state law sometimes required health

127. *Id.* at 562.
128. Strahilevitz, *supra* note 80, at 939–46.
129. 533 U.S. 27, 34 (2001).
130. 532 U.S. 67, 76 n.9 (2001).

professionals to inform the police of evidence of criminal conduct they obtained while providing medical care to their patients.[131] While both cases remain good law, the more common approach in Fourth Amendment cases is the third-party doctrine, which holds that individuals who share information with anyone should expect that it will be shared with the government, regardless of the ex ante probability that such sharing will in fact occur.[132]

The *Maynard* court borrowed from tort reasoning and took the idea of "reasonable expectations of privacy" far more literally than cases applying the third-party doctrine do.

> [T]he information the police discovered in this case – the totality of Jones's movements over the course of a month – was not exposed to the public: . . . unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe those movements is effectively nil.[133]

In footnotes, the court emphasized an article written in this law review in 1954 by the Chief of the Los Angeles Police Department noting that constant surveillance is "not only more costly than any police department can afford, but in the vast majority of cases it is impossible."[134]

The question of whether Fourth Amendment "reasonable expectations of privacy" should resemble the reasonable expectations of privacy that are referenced in tort law and many other areas of information privacy law is a difficult one. Several factors make the question a hard one. I will flag two here. First, as a historical matter the Fourth Amendment's enactment preceded the Warren and Brandeis privacy revolution. Second, the dramatic nature of the exclusionary rule remedy—which may result in a guilty perpetrator walking free—may make courts especially resistant to conclusions that reasonable expectations of privacy exist, even in those settings where they would be less hostile to finding a reasonable expectation in the context of interactions between non-state actors.[135] These reasons, and others that I hope to explore at greater length elsewhere, warrant against blindly translating "reasonable expectations of privacy" that have been recognized in tort to Fourth Amendment contexts. Conspicuously, I do not advocate reunifying the Fourth Amendment with privacy tort law here.

---

131. *Id.* at 78 n.13.

132. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976).

133. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010).

134. *Id.* at 565 n.7 (citing W.H. Parker, *Surveillance by Wiretap or Dictograph: Threat or Protection?*, 42 CALIF. L. REV. 727, 734 (1954)).

135. For helpful discussion, see Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119 (2002); David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 207–10 (2002); and William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016 (1995).

Maynard, though, does not take the position that reasonable expectations of privacy in tort law, FOIA, and other non-Fourth Amendment contexts are the same as those arising under the Fourth Amendment. It only takes the position that such precedents are instructive, and can be used to get a handle on the Fourth Amendment issues presented by relatively novel technologies. In that sense it is a model of common-law judging, drawing on existing domestic precedents, and scrutinizing them to see how analogous they are to the case at hand. To be sure, GPS surveillance of vehicles is an issue about which people's actual expectations of privacy are in flux. New applications are being developed daily for GPS-enabled smartphones, and many consumers seem eager to broadcast information about their movements.[136] In the near future practical anonymity of drivers on roadways may be eroded by crowd-sourced "How's My Driving?" technologies, and there are many reasons to believe that, on balance, this loss of motorist anonymity would be a good thing.[137] Reasonable minds therefore might quarrel with the result in *Maynard*, but the methodology is a genuine breakthrough, and exactly the sort of thing I have in mind when I advocate information privacy law's reunification.

Perhaps the Supreme Court will follow in the D.C. Circuit's footsteps. There is a golden opportunity to do so this Term. On March 8, 2010, the Supreme Court granted certiorari in *NASA v. Nelson*. To privacy scholars, this was a stunning turn of events. It has been thirty-three years since the Supreme Court has said a word about the constitutional right to information privacy. But *Nelson* is a case in which the constitutional information privacy claims are the only issues present on appeal. In granting certiorari, the court accepted an invitation by Chief Judge Kozinski, whose dissent from the denial of a rehearing en banc ended as follows:

> [T]here are circumstances when a well-worn doctrine can grow into "a vexing thicket of precedent" that then becomes "difficult for litigants to follow and for district courts—and ourselves—to apply with consistency." . . . The back and forth between the panel and my dissenting colleagues illustrates that we have reached this point with the doctrine of informational privacy. Though I am sympathetic to the arguments of my dissenting colleagues, it's not clear that the panel has misapplied circuit law; when the law is so subjective and amorphous, it's difficult to know exactly what a misapplication might look like.
>
> It's time to clear the brush. An en banc court is the only practical way we have to do it. We didn't undertake that chore today, but we'll have to sooner or later, unless the Supreme Court should intervene.[138]

---

136. *See, e.g.*, Miguel Helft & Jenna Wortham, *Facebook Unveils a Service to Announce Where Users Are*, N.Y. TIMES, Aug. 18, 2010, http://www.nytimes.com/2010/08/19/technology/19facebook.html.

137. *See* Lior Jacob Strahilevitz, *"How's My Driving?" for Everyone (and Everything?)*, 81 N.Y.U. L. REV. 1699 (2006).

138. Nelson v. NASA, 568 F.3d 1028, 1054 (9th Cir. 2009) (Kozinski, C.J., dissenting

Intervene it has. In these last few pages, I want to recommend a concrete way for the Court to clear the brush and bring some semblance of sanity to the constitutional right of information privacy, and to information privacy law more generally. By working our way through *Nelson* itself, we can see ways in which the law of privacy might be reunified. In this case, that means recognizing that the constitutional right to information may have to disappear.

Nelson involves the federal government's use of detailed background checks to investigate the suitability of Jet Propulsion Laboratory (JPL) employees for continued employment. The plaintiffs represent a class of JPL scientists, engineers, and administrators who are classified by NASA as "low risk" employees because their jobs "do not involve policymaking, major program responsibility, public safety, duties demanding a significant degree of public trust, or access to financial records with significant risk of causing damage or realizing personal gain."[139] Under new federal regulations, even longtime JPL employees were to be subjected to background checks in which government agents would ask employees, their references, their prior employers, and their landlords questions about whether they had: used drugs or undergone treatment or counseling for drug addiction in the last year; used abusive language; been involved in personality conflicts; developed mental, emotional, psychological, or psychiatric issues; or engaged in sodomy. In addition, third parties would be asked whether they knew anything, good or bad, about the JPL employees that would be relevant to their ability to work for the government.[140] The applicable guidelines stated that having engaged in sodomy did not present problems with respect to suitability for government employment, but that investigators were to examine employees' susceptibility to coercion or blackmail based on their having engaged in sodomy.[141]

The district court denied the plaintiff's request for an injunction, but the Ninth Circuit reversed with respect to the government's inquiries about drug treatment (as opposed to drug use) and open-ended "investigation[s] of the most private aspects of class members' lives."[142] While the court held that the government's inquiries into its employees' backgrounds were legitimate, it applied intermediate scrutiny and held that the government's investigations were not narrowly tailored to further these legitimate interests.[143] The court emphasized the fact that the background checks were to be applied, not only to job applicants, but to employees who had performed admirably for decades at JPL, which the court thought greatly magnified the privacy harm.[144]

---

from the denial of rehearing en banc).

139. *Id.* at 1029 n.3 (Wardlaw, J., concurring in the denial of rehearing en banc).

140. *Id.* at 1032–33.

141. *Id.* at 1033.

142. *Id.* at 1032; Nelson v. NASA, 530 F.3d 865, 879 (9th Cir. 2008).

143. *Nelson*, 568 F.3d at 1032.

144. *Id.* at 1035, 1037.

As the judges debated whether to consider the case en banc, several disagreements emerged. The most important for the purposes of this Article was the question of how privacy precedents from other branches of privacy law jurisprudence should inform constitutional right of information privacy doctrine. To one of the dissenters, Judge Callahan, a unified approach was sensible:

> The panel's opinion concludes that individuals have a constitutionally protected right to privacy in information disclosed to third-party employment references. No other court has held as much, and for good reason—the Supreme Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties. . . . Absent some privilege . . . an applicant does not have an expectation of privacy to information disclosed by a reference.
>
> The panel concludes that Fourth Amendment case law defining whether an individual has an expectation of privacy over information that he has already disseminated to the public is not the proper focus in the evaluation of information privacy rights and contends that, instead, we should focus on the general nature of the information sought. Although I agree with the panel that the constitutional right to informational privacy is not limited to Fourth Amendment searches, I disagree with the suggestion that whether an individual has an expectation of privacy under a constitutional right to informational privacy is not informed by Supreme Court case law interpreting an expectation of privacy under the Fourth Amendment. In fact, one of the Supreme Court's first decisions recognizing a constitutional right to informational privacy specifically cited to Fourth Amendment case law in defining this right.[145]

The judges concurring in the denial of a rehearing, by contrast, insisted that the Fourth Amendment third-party-doctrine cases provided no guidance in a constitutional right to information privacy case. As they saw it:

> [T]he right to informational privacy and Fourth Amendment rights are not fully coextensive. . . . [A]lthough in the Fourth Amendment context there is a general principle "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties, 'the legitimate expectation of privacy' described in this context is a term of art used only to define a search under the Fourth Amendment, and *Miller* and *Smith* do not preclude an *informational privacy* challenge to government questioning of third parties about highly personal matters."[146]

---

145. *Id.* at 1044 (Callahan, J., dissenting from the denial of rehearing en banc) (citations omitted).

146. *Id.* at 1031 n.7 (Wardlaw, J., concurring in the denial of rehearing en banc) (citations omitted).

The back and forth between Judges Callahan and Wardlaw is deeply unsatisfying. Judge Callahan says privacy law should be unified because the Ninth Circuit should not do something inconsistent with what the Supreme Court has done. Judge Wardlaw's response is that inconsistency with other branches of privacy law is a non-issue. To her the only privacy cases that matter are constitutional right to information privacy cases. While this Article is sympathetic to Judge Callahan's premise that privacy law's different parts ought to be consistent and coherent, her execution of the reunification project leaves something to be desired. A more forceful expression of her view would have emphasized the most counterintuitive aspect of the majority's holding, which is that in a case involving overlap between the Fourth Amendment and the constitutional right to information privacy, the right that the Supreme Court has never embraced and that has only the faintest grounding in the constitutional text would be the one that provides an aggrieved citizen with the most robust and far-reaching constitutional protection.

That said, there is a large body of privacy law beyond the Fourth Amendment, and it, too, has addressed the question of whether it is a violation of privacy to ask an individual's friends and former employers about her past behavior, her mental health issues, her sexual preferences and the like. The issue has come up in tort cases, where some courts have held that such inquiries do not amount to an intrusion upon seclusion. A leading American case that embraces a "third party doctrine" approach to tort law is *Nader v. General Motors*, in which the New York Court of Appeals held that General Motors' very intrusive interviews of Ralph Nader's associates and friends were not an intrusion upon seclusion.[147] This was true even though General Motors' agents misrepresented their purpose—claiming to be working on behalf of an entity that was considering hiring Nader, when in actuality General Motors hoped to intimidate or discredit the plucky young author of *Unsafe at Any Speed.*

Of course, the facts of *Nelson* arose in California, where privacy law has by-and-large rejected *Nader*'s extension of the third-party doctrine to tort law.[148] As it happens, California is the rare American jurisdiction where privacy tort law and constitutional privacy law have essentially merged—thanks to the California Constitution's privacy clause, which lacks a state action requirement.[149] As a result, many privacy cases that could be brought

147. 255 N.E.2d 765 (N.Y. 1970).

148. For a lengthier discussion of the case law, see Strahilevitz, *supra* note 80, at 939–46.

149. CAL. CONST., art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); Huntingdon Life Scis., Inc. v. Stop Huntingdon Animal Cruelty USA, 29 Cal. Rptr. 3d 521, 546 (Cal. Ct. App. 2005) (noting that the state constitution protects against invasions of privacy by state and non-state actors). The merger of constitutional and tort privacy protections in California is a recent phenomenon, which *Huntingdon* hinted at and a more recent case confirmed. Compare the 1998 case of *Shulman v. Group W Prods., Inc.*, 955 P.2d 469, 487 (Cal. 1998) ("Nothing in *Hill* or our

under a tort theory are brought under the state constitution, and the welfarist balancing test that Judge Posner subtly introduced in *Desnick* has been explicitly embraced in the doctrine.[150]

Some of those cases interpreting the California Constitution do embrace a result that is consistent with the Ninth Circuit's ruling in *Nelson*. For example, the California Supreme Court held in 1986 that requiring public employees to submit to polygraph testing in order to investigate a specific crime violated the employees' privacy rights under the state constitution.[151] Another 1991 opinion, albeit one that was mooted on appeal, held that Target's use of a "Psychscreen" program, a psychological profiling device that required job applicants to answer questions about their religious beliefs and sexual orientation, violated the applicants' rights under the California Constitution.[152]

On the other hand, a 1994 California Supreme Court case found that the NCAA's drug testing of collegiate athletes did not violate the California Constitution's privacy protections, though that opinion did focus on the peculiarities of athletic competition and reserved judgment on how its ruling should apply to workplace settings.[153] Moreover, the state courts have rejected one of the central rhetorical arguments put forward by the *Nelson* court, which is that employees have much stronger privacy protections than mere job seekers.[154] It is strange that the California and federal constitutions should differ on such a question. Fascinatingly, the *Nelson* panel opinion engaged in essentially no exploration of applicable state law while exploring the federal constitutional question.

This review of the case law brings us to a surprising place. Were anyone other than the federal government the defendant, the plaintiffs in *Nelson* could have prevailed had they pursued a tort or constitutional claim. Under California tort law, sharing information with friends and associates does not necessarily waive reasonable expectations of privacy against the information being shared with outsiders.[155] And under closely connected state constitutional law,

---

more recent constitutional privacy cases, however, suggests that the conceptual framework developed for resolving privacy claims was intended to supplant the common law tort analysis or preclude its independent development.") with the 2009 case of *Hernandez v. Hillsides, Inc.* 211 P.3d 1063, 1073–74 (Cal. 2009) ("The right to privacy in the California Constitution set standards similar to the common law tort of intrusion. . . . We will assess the parties' claims and the undisputed evidence under the rubric of both the common law and constitutional tests for establishing a privacy violation. Borrowing certain shorthand language from *Hill*, which distilled the largely parallel elements of these two causes of action, we consider (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests.").

150. *Hernandez*, 211 P.3d at 1074.

151. Long Beach City Emps. Ass'n v. City of Long Beach, 719 P.2d 660, 670 (Cal. 1986).

152. Soroka v. Dayton Hudson Corp., 18 Cal. App.4th 1200, 1214 (Cal. Ct. App. 1991), *dismissed as moot and superseded by* 862 P.2d 148 (Cal. 1993).

153. Hill v. NCAA, 865 P.2d 633, 664 (Cal. 1994).

154. *Id.* at 1210.

155. Times Mirror Co. v. Superior Court, 244 Cal. Rptr. 556, 560–61 (1988).

employers are likely prohibited from asking questions about sexual orientation, and perhaps about drug treatment as well. Of course, thanks to the federal Constitution's Supremacy Clause, a state constitutional claim challenging the federal regulations is a non-starter. Plaintiffs could still sue the federal government under a tort theory, given the sovereign immunity waiver in the Federal Tort Claims Act.[156] In light of the California Supreme Court's recent holding that state tort law and the California Constitution provide equivalent protection, the expansive precedents arising under the state constitution could be employed by a plaintiff suing under the Tort Claims Act. But discretionary function immunity would almost certainly permit the government to escape liability.[157]

The Supreme Court may well decide in *Nelson* that there is no such thing as a constitutional right to information privacy. The Sixth Circuit has said as much, and the D.C. Circuit has leaned in that direction, though every other circuit court to consider the issue has come out the other way. An abolitionist approach would view the sorts of harms to privacy interests that arose in *Nelson* as ordinary tort harms that are appropriately pursued through ordinary tort causes of action. To be sure, under the Federal Torts Claims Act's due care doctrine a tort cause of action against the federal government on the facts of *Nelson* is a probable loser, but that reflects a congressional judgment about the sorts of government actions that ought not to engender liability. The primary appeal of removing these questions from constitutional law relates to error-correction: if the judges make a mistake in deciding difficult, subjective questions of privacy law in areas where the law, technology, and norms are in a constant state of flux, or if the legislature immunizes conduct that the citizenry believes ought to be actionable, those errors can be fixed via ordinary legislation at the state or federal level rather than through the cumbersome processes of amending the federal Constitution or changing the composition of the Court through appointments.

In contrast to *Nelson* and *Whalen* many of the landmark constitutional right to information privacy cases involve state governmental defendants and could have been brought under a state tort or state constitutional theory. One prominent example would be a case like *Doe v. Borough of Barrington*.[158] In that case, an arrestee with bleeding lesions disclosed his HIV-positive status to police officers taking him into custody so that they could take appropriate precautions to protect themselves from infection. A member of the same police department subsequently and improperly informed the arrestee's neighbors of his HIV status. A panic ensued, causing various neighbors to pull nineteen

156. Qualified immunity would not present a significant obstacle to the suit, at least where the law was reasonably well developed. *See* Castro v. United States, 34 F.3d 106, 111 (2d Cir. 1994).

157. *See, e.g.*, 28 U.S.C. § 2680(a) (2006); Welch v. United States, 409 F.3d 646, 652–54 (4th Cir. 2005).

158. 729 F. Supp. 376 (D.N.J. 1990).

children out of the public school attended by the arrestee's children for fear of them contracting the disease through casual conduct. A media report on the panic then disclosed Doe's real name.[159]

The court understandably ruled in Doe's favor, and *Barrington* is included as a principal constitutional right to information privacy case in Solove and Schwartz's privacy law casebook.[160] But Doe did bring pendent state tort invasion of privacy claims under New Jersey law,[161] and those claims would have fared well, given the defendants' apparent lack of good faith in exercising their official duties.[162] The New Jersey Tort Claims Act permits causes of action for invasion of privacy to be asserted against the government.[163] And New Jersey, along with most states, recognizes the tort for public disclosure of private facts.[164] A plaintiff would have less luck in a jurisdiction like North Carolina, which prohibits invasion of privacy tort suits against the state and which lacks a California-style state constitutional provision to permit tort-like claims to proceed in the state courts.[165]

In any event, the approach of killing off the constitutional right of information privacy creates what I call the Bobby Ewing dilemma. The television show *Dallas*'s entire eighth season, which followed the death of protagonist Bobby Ewing, was revealed to be a mere dream sequence. After Patrick Duffy (who played Bobby) agreed to return to the show, his wife/widow awoke to find her husband in the shower, delighted to learn that she had dreamed an entire season's worth of melodramatic content. Viewers of the show were less pleased.

In two 1977 cases, the U.S. Supreme Court devoted pages and pages of the U.S. Reports to discussing the constitutional right to information privacy before deciding that neither the *Whalen* plaintiff nor Richard Nixon had a winning case under the right. In the decades since, the appellate courts have considered hundreds of cases involving the right and developed a great deal of (unsatisfying) doctrine in an effort to flesh it out. Declaring the non-existence of such a right after all this time will look bad, even if the right in question is one about which the legal profession and general public know little.

The basic question presented in *Nelson*, then, is who should decide on the remedies for government conduct that would be tortious if engaged in by a private party. The *Nelson* panel thought that the federal courts interpreting the federal Constitution should decide, whereas Judge Callahan's dissent implies that these questions should be addressed to Congress, the state courts, and state

159. *Id.* at 379.
160. SOLOVE & SCHWARTZ, *supra* note 18 at 479.
161. *Barrington*, 729 F. Supp. at 379.
162. Toto v. Ensuar, 952 A.2d 463, 469–70 (N.J. 2008).
163. Leang v. Jersey City Bd. of Educ., 969 A.2d 1097, 1107, 1115–17 (N.J. 2009).
164. Romaine v. Kallinger, 537 A.2d 284, 297 (N.J. 1988).
165. *See* Toomer v. Garrett, 574 S.E.2d 76, 91 (N.C. App. 2002).

legislatures. Superficially, either approach can be squared with an attempt to reunify privacy law. A more persuasive version of the panel's "preservationist" approach would view state tort law (and state constitutional law, in California) as persuasive authority with respect to the question of what the federal Constitution should mean. This achieves coherence in the law of any particular place, but does create the disturbing side effect that the federal Constitution would be more protective in some jurisdictions than others because of variations in tort law. We would just be replacing incoherence with reified inconsistency.[166] Having said that, if common law tort precedents are permitted to influence constitutional rights, then many of the ordinary concerns about creating constitutional rules when statutory or common law rules will suffice are blunted. The abolitionist approach, by contrast, would create coherence by withdrawing the federal Constitution from the domain of information privacy protections—leaving federal statutes, state tort laws, and state constitutional doctrine to remedy (or refuse to remedy) these sorts of claims.

For the sake of coherence, and to promote the development of tort law, statutory, or state constitutional remedies, it would be best to end the constitutional right to information privacy experiment. But if the Court must breathe new life into the prodigal constitutional right, it could adopt a "second best" approach—treating the constitutional right as a gap filler in those settings where federal statutory or state law remedies are unavailable for serious wrongs. The tort inquiry would either inform the constitutional inquiry, as in *City of Artesia*, or become fully harmonized with the constitutional inquiry, which seems to have happened under the California Constitution's right to privacy.[167] Under such an approach, the Constitution would prompt the courts to ask variations on the familiar tort questions: Has the government infringed upon its employees' private matters or concerns? Is the government's conduct a clear violation of existing social norms? Does the gravity of the privacy harm to the plaintiffs and those similarly situated exceed the societal benefits? Affirmative answers to all three questions would point toward the violation of the constitutional right. In the process, the law of information privacy would be judged toward uniformity through the creation of a federal right with content that did not vary by jurisdiction. Thirty-three years is a long time for an experiment, and enough time to determine that the experiment has not turned out well. *Chao* suggested that the Supreme Court was interested in beginning the project of returning coherence to information privacy law, and *Nelson* can provide further momentum for the long overdue rationalization of American privacy law.

166. I use the word "reified" because constitutional rights presently do vary between, say, the Sixth Circuit, which recognizes no constitutional right of information privacy, and most other circuits, which do. *See supra* text accompanying note 28.

167. *See supra* text accompanying notes 44–47 (discussing *Artesia*) and note 149 (discussing the cases interpreting the California Constitution).