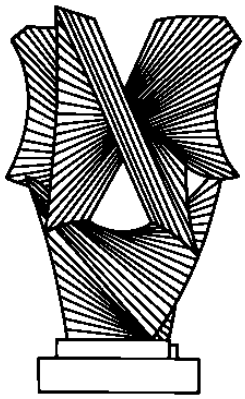
2010

Reunifying Privacy Law

Lior Strahilevitz

CHICAGO

PUBLIC LAW AND LEGAL THEORY WORKING PAPER NO. 309



REUNIFYING PRIVACY LAW

Lior Jacob Strahilevitz

THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

May 2010

Reunifying Privacy Law

Lior Jacob Strahilevitz*

forthcoming in 98 *California Law Review* ___ (2010)

Abstract

In the years since Samuel Warren and Louis Brandies 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 paper argues for the reunification of 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 paper examines how this reunification project can be accomplished, why it is desirable, and whether it is consistent with the Supreme Court's methodological guidance in privacy controversies.

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

* Deputy Dean, Professor of Law & Walter Mander Teaching Scholar, University of Chicago Law School. Thanks to Rosalind Dixon, Lee Fennell, Tom Ginsburg, Tom Gorman, Mike Hintze, Aziz Huq, Saul Levmore, Richard McAdams, Martha Nussbaum, Adam Samaha, David Strauss, Matt Tokson, faculty workshop participants at the University of Chicago Law School, and participants in U.C. Berkeley's Prosser at Fifty Symposium for comments on an earlier draft, to Katie Heinrichs for research assistance, and the Morton C. Seeley Fund and Milton and Miriam Handler Foundation for research support.

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 up 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. Many of the most important developments took place entirely independent of his work and ideas. But Prosser was the first scholar to notice privacy law's fragmentation, and he lent it his influential stamp of approval. His argument for fragmentation was opposed by some contemporaries,[1] but it was Prosser who has 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 fit with the newly fragmented common law in a coherent way. We should suspect that the common law fragmentation influenced the subsequent statutory fragmentation, though supporting this suspicion with hard evidence is a tall order.

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 German'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.

Neither was the fragmentation of privacy law inexplicable. But it was 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, and this paper will make the case for returning the law to its 1890 origins, an era in which the law was sparse but coherent. I will 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 inferior 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 paper concludes by examining the two ways in which *Nelson v. NASA* can be decided so as to promote 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

[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 was undermining the important conceptual work that Warren and Brandeis had done. He also argued, contrary to Prosser, that a single societal interest – human dignitary interests – undergirded all invasion of privacy claims.

commonalities with information privacy law,[2] I believe the stark differences in the respective analytical frameworks, stakes, historical pedigrees, and distributive contexts 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. The question of whether Fourth Amendment "reasonable expectations of privacy" should resemble the reasonable expectations of privacy that are referenced in many other areas of information privacy law is a much more difficult one. This paper largely leaves for later work the question of whether it is appropriate to create coherence between Fourth Amendment law and the bodies of information privacy law discussed herein.[3] At the same time, the paper also accepts the argument, put forward at great length elsewhere, that information privacy is a category with enough commonalities to render it a coherent concept.[4]

The paper 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 the tort 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 sections 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 and privacy tort law overlap substantially. It is therefore unnecessary to have two separate doctrines to deal with the problem of privacy invasions perpetrated by the state and a genuine puzzle as to 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, 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 suggests that while the Supreme Court lacked a compelling justification for holding that "unwarranted invasions of personal privacy" could mean very different things 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 what counts as an invasion of privacy under FOIA.

---

[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).

[3] The question is made difficult by several factors. 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. For helpful discussion, see 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).

[4] *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);

Part IV shows how the Privacy Act can be reconciled with other aspects of information privacy law. It offers a new defense of the Supreme Court's leading privacy precedent, *Doe v. Chao*. The paper 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 by inoculating the government against a significant threat posed by lower court decisions interpreting the Privacy Act in a manner that would impose substantial liability on the government even for disclosing information that is 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. The first is that more coherent law will lower the compliance costs faced by firms and individuals. The second is that more coherent law will improve the quality of common law adjudication by reducing uncertainty about how the law will treat particular controversies. The third is that more coherence will help equalize the treatment of similarly situated parties.

Part VII concludes with the most urgent part of the paper. In March, the Supreme Court granted certiorari 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 paper 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 of information privacy doctrine, there are two viable paths for the Court to walk down. One would enhance coherence in privacy law by holding that there is no such thing as a constitutional right of information privacy, holding that the problems confronted in those category of cases are most appropriately dealt with via garden variety tort suits. The second approach would regard the constitutional right of information privacy as a useful gap filler to be applied where political pathologies suggest that legislative processes do not adequately vindicate privacy interests. If the constitutional right to information privacy is to persist, it ought to much more closely resemble privacy tort law—and 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 are the right questions for courts to be asking in constitutional adjudication. For reasons explained in the paper, path one seems more attractive to path two, which in turns seems far superior to the continued development of a *sui generis* constitutional right of information privacy.

I.

Let us begin with tort law and the two most influential American pieces of privacy scholarship. In their 1890 article, *The Right to Privacy*, 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, and some of their examples focused on the dissemination of said information.[5]

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.[6]

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. The two torts that receive the lengthiest treatment in Prosser (and that seem most closely tied to privacy itself) are intrusion upon seclusion and public disclosure of private facts. Although one tort deals with information gathering and the other deals with information dissemination, the public disclosure tort circumscribes the intrusion tort. That is to say, 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 do.[7]

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 offensive to a reasonable person. The public disclosure tort also requires (1) intentional conduct by the defendant,[8] and the (2) disclosure of private facts or affairs concerning another person. If a fact is private for the purposes of the intrusion tort, it is private

---

[5] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 295-96, 201-02 (1890)

[6] *Id*. at 215.

[7] *See*, *e.g.*, Trammell v. Citizens News Co., 148 S.W.2d 708 (Ky. 1941).

[8] Some jurisdictions contravene the Restatement by recognizing negligent invasions of privacy, both via intrusion upon seclusion and public disclosure of private facts. If a jurisdiction requires intentionality for intrusion it does so for public disclosure as well. *Compare* Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702 (DC 2009) (no negligent invasion of privacy liability); Hudson v. S.D. Warren Co., 608 F. Supp. 477, 481 (D. Me. 1985) (no negligent invasion of privacy liability); Bailer v. Erie Ins. Exch., 682 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. 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 App. 1985) (same). Texas authorities are currently split over whether negligent invasion of privacy claims are permitted. *See* Doe v. Mobile Video Tapes, Inc., 43 S.W.3d 40, 53-53 (Tex. App. 2001).

for the purposes of the public disclosure tort, and vice versa. Along the same lines, (3) the "highly offensive" nature of the defendant's conduct must be manifest in either tort. Though 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, this fine distinction often eludes them.[9]

Critically, Prosser's public disclosure of private facts tort requires two more elements: publicity and non-newsworthiness. An intrusion upon seclusion is not dependant on the defendant sharing private information with anybody else. There are cases in which the plaintiff recovered even though the defendant is the only person who might have learned the private information.[10] But cases in which there is an intrusion upon seclusion by one or two people, but no subsequent publicity, are rarely brought because the damages resulting from such harm are typically low.

The final element—non-newsworthiness—ostensibly provides the most salient difference between public disclosure and intrusion. 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.[11] But is it followed in practice? Perhaps not.

Arguably the most famous pair of American privacy tort law opinions are the Ninth Circuit's 1971 opinion in *Dietemann v. Time* and the Seventh Circuit's 1995 opinion in *Desnick v. ABC*.[12] Among the privacy casebooks, Solove and Schwartz prominently pair the cases side by side, and Allen compares them early in her casebook too, though she devotes more space to *Dietemann*.[13]

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 pled nolo contendre, based on the photographs and recordings made by the reporters.[14]

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

[9] Restatement (Second) of Torts § 652(B).

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

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

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

[13] ANITA L. ALLEN, PRIVACY LAW AND SOCIETY 47-50 (2007); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 84-89 (3rd ed. 2009).

[14] *Dietemann*, 449 F.2d at 245-47.

recommended that several of them undergo cataracts surgery.[15] The broadcast of the ABC story on Dr. Desnick's practices evidently contributed to his leaving the profession.[16]

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 "the 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."[17] 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 Radiohead "pay what you want" business model instead of fixed prices. Coffee shops sometimes charge customers whatever they are willing to pay, but businesses they remain.[18] 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 would sympathize, and which is suggested in early portions of his opinion, especially its charming discussion of restaurant critics.[19] 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 promoting free conversations.

As a pragmatic defense of the divergent results, this analysis makes a great deal of 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 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.

---

[15] *Id*.

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

[17] *Desnick*, 44 F.3d at 1353.

[18] *See, e.g.*, Amy Roe, *A Kirkland Café with No Prices*, Seattle Times, February 6, 2007; Josh Tyrangiel, *Radiohead Says: Pay What You Want*, Time, October 1, 2007.

[19] *Desnick*, 44 F.3d at 1351-52.

II.

In *Whalen v. Roe*[20] the Supreme Court assumed for the sake of argument that the United States Constitution protected individuals against the improper collection, aggregation, or disclosure of their private information. It then held that even 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.[21] The Court then lost interest in the constitutional right of information privacy for the past 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 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 there is any such thing as a constitutional right of information privacy, given the poorly developed nature of the Supreme Court's jurisprudence. Among the circuit courts that have recognized such a constitutional right, the Third Circuit's law is best-developed.

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*.[22] 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. 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 what the proper cause of action is. In some jurisdictions, sovereign immunity prohibits an individual from suing the state for invasion of privacy.[23] In other jurisdictions, sovereign immunity imposes no such bar because it has been waived via the

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

[21] Nixon v. Administrator of General Serv., 433 U.S. 425 (1977).

[22] 638 F.2d 570 (3d Cir. 1980). *Westinghouse* has been cited more than one thousand times as of 2010.

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

state's applicable Torts Claims Act.[24] Federal cases typically construe the federal Torts Claims Act as having waived sovereign immunity in invasion of privacy tort suits against the federal government,[25] though limited exceptions apply. For example, if the post office's improper delivery of mail invades someone's privacy, then the federal Torts Claims Act does seem to bar the action—an explicit provision immunizing the post office from suits prevails over the Act's silent implication that the federal government has waived sovereign immunity in invasion of privacy suits.[26] Moreover, several states have enacted their own versions of the federal Privacy Act, which may provide an alternative basis for recovery.[27] 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 whom within that government has engaged in the wrongful conduct.

The case law thus creates a strange set of circumstances. Suppose that a governmental employee living in Ohio has his HIV status improperly disclosed by his supervisor to all his co-workers—a fact pattern that has given rise to much litigation. Ohio permits suits for intentional or negligent invasions of privacy.[28] 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.[29] He will be able to recover under an invasion of privacy theory even though the defendant's conduct is unintentional. 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.[30] But he probably cannot sue the same employer under the constitutional right of information privacy—again, there is a D.C. Circuit opinion on point.[31] 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.[32]

---

[24] *See, e.g.*, Wadman v. State, 510 N.W.2d 426, 429-30 (Neb. App. 1993).

[25] *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).

[26] *See* McCullough v. United States, 2004 WL 2029985, at **1 (2d Cir. Sep. 10, 2004) (unpublished).

[27] *See infra* note 56.

[28] See *supra* note 8.

[29] There is no sovereign immunity for invasion of privacy suits when the act complained of arises out of an employment relationship with the subdivision itself Ohio R.C. 2744.09(B), though this rule may not apply to intentional invasions of privacy. See Nungester v. Cincinnati, 654 N.E. 2d 423, 427 (Ohio App. 1995). There is also the added complication of the Ohio Privacy Act under R.C.1347.10, which seems to allow a waiver of sovereign immunity for invasion of privacy claims, but this is statutory and not common law invasion of privacy. This interaction between the Privacy Act and the Political Subdivision Tort Immunity Act is discussed in *Ross v. Trumbull City. Child Support Enforcement Agency*, 2001 WL 114971 (Ohio App. 2001).

[30] *Black*, 564 F.2d at 531.

[31] American Federation of Government Employees, AFL-CIO v. Dept. of Housing & Urban Development, 118 F.3d 786, 791-93 (D.C. Cir. 1997)

[32] *See, e.g.*, Alexander v. Peffer, 993 F.2d 1348 (9th Cir. 1993) (recognizing the constitutional right to information privacy, but finding that disclosure by the City of Omaha Police Department of her unsuccessful application to become a police officer was not a constitutional violation because it was not private information).

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.[33] Where the government is the defendant, the harm to the plaintiff is the same regardless of the theory being pursued. Yet, in formulating a doctrine that deviates sharply from privacy tort law, the *Westinghouse* court never explained what it was up to. 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*. 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.[34] The complaint further alleged that the plaintiff was socially shunned by co-workers after the disclosure, though he continued to be 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 employer, who were on a need-to-know basis. The information was publicized at his workplace, resulting in his social marginalization. The disclosure to co-workers was not newsworthy, since 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.[35] All the elements of a tort are satisfied. Yet the court nevertheless 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 of information privacy.[36] The counterpart to Judge Posner's reunifying opinion in *Desnick* is *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.[37] The court began its analysis with language that seems totally straightforward, but which subverts the 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."[38] The court then reviewed common law precedents holding that

---

[33] The Washington Supreme Court has held, quite sensibly, that where cognizable common law invasion of privacy claims and constitutional privacy claims are being 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.

[34] Doe v. SEPTA, 72 F.3d 1133, 1135-36 (3rd Cir. 1995).

[35] Multimedia WMAZ v. Kubach, 443 S.E.2d 491 (Ga. 1994).

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

[37] Smith v. City of Artesia, 772 P.2d 373 (N.M. App. 1989).

[38] *Id*. at 374.

the deceased have no privacy rights and constitutional rulings inconsistent with the idea that someone could have a privacy interest in another individual.[39] But by beginning with existing tort law doctrines, the law biased its opinions toward uniformity, not fragmentation.

Fascinatingly, the United States Supreme Court in *National Archives and Records Administration v. Favish* also looked to some common law precedents to determine whether Vince Foster's relatives had a privacy interest in his autopsy photographs under the Freedom of Information Act's (FOIA's) privacy exemptions.[40] 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.[41] 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. 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.

Let us 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 was almost entirely silent as to the meaning of the statutory language in exemption 6 (permitting the withholding of "personal and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy") 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").

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.[42] But writing in the *Journal of Legal*

[39] *Id*. at 374-75.

[40] National Archives and Records Admin. v. Favish, 541 U.S. 157 (2004).

[41] 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)).

[42] *See, e,g.*, Perkins v. Freedom of Information Commission, 635 A.2d 783, 788-91 (Conn. 1993); Hearst Corporation v. Hoppe, 580 P.2d 246, 252-54 (Wash. 1978); Harris v. Cox Enterprises, 348 S.E.2d 448 (Ga. 1986); Webb v. Shreveport, 371 So.2d 316 (La. Ct. App. 1979); State Employees Assn. v. Dept. of Management & Budget, 404 N.W.2d 606 (Mich. 1987); Jordan v. Motor Vehicles Division, 781 P.2d 1203 (Or. 1989); Industrial Foundation

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.[43] Although it did not cite this specific language in Kronman's article, the Supreme Court in *Reporter's Committee* did both cite other portions of the Kronman article and hold that the question of whether a disclosure was an 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.[44]

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 come up with a satisfying explanation for the divergence. It may well be the case 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 what it can say itself.[45] That dynamic suggests that we might view FOIA privacy and tort privacy differently, perhaps removing non-newsworthiness as a consideration in FOIA privacy disputes. 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 typically 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 a 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.[46] 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 about the importance of enabling people to trust

---

v. Texas Accident Board, 540 S.W.2d 668 (Tex. 1976); Child Protection Group v. Cline, 350 S.E.2d 541 (W. Va. 1986).

[43] Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 9 J. Legal Studies 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.").

[44] *Reporter's Committee*, 489 U.S. at 762 n.13 & 772 n.20.

[45] Note that there is some constitutional law compelling citizen access to government information.

[46] A robust Privacy Act may be part and parcel of the same concern.

private actors—be they friends, co-workers, 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 make a difficult empirical and / or normative case to support such a distinction. To date, neither courts nor commentators have made such a case.

A more serious objection 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, etc. 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 information about themselves to private entities than to the state.[47] Much of the information in the government's hands is information that high-level policy makers don't realize exists, that is poorly organized, and 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.[48]

To be sure, the private sector in the United States is not bound by any equivalent to FOIA. If you ask Goldman Sachs to provide you with information about its operations, they can say no to your request—or ignore you completely—without having to provide a privacy rationale or any other justification. They certainly needn't show that the disclosure would constitute a tort if they wish to rebuff your request. But that contrast with FOIA is 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 the FOIA's subsidiary purposes (protecting privacy) at the expense of its overarching purpose (promoting disclosure).

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 landmark FOIA privacy cases. In *Reporter's Committee*, the Supreme 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. 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

[47] 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).

[48] 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.

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 v. Sullivan*. By rejecting privacy tort law's principles, *Reporter's Committee* arrives at a result quite hostile to free speech interests—it is a result that surely would have distressed Warren and Brandeis.[49]

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. 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.[50] 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 injuries,[51] and that resistance would have to be stronger still in the case of a suicide victim who chose to kill himself in a public place. 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 significant mistakes 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

---

[49] Warren & Brandeis, *supra* note , at 214-15.

[50] See cases cited *supra* note 41. A very recent case, *Catsouras v. Department of California Highway Patrol*, 181 Cal.App.4th 856 (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. *See id.* at 870-72. The intermediate appellate court should be faulted for failing to consider the 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. *See infra* text accompanying note 51.

[51] Shulman v. Group W. Productions, Inc., 955 P.2d 469, 490 (Cal. 1998).

is not just a problem for those who would like to see conceptual clarity in the law—it results in outcomes that impede significant speech interests as well.

IV.

The federal Privacy Act 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.[52] 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.

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."[53] The law defines a 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."[54] 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.[55] Yet 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."[56] 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 case is *Quinn v. Stone*.[57] The case involved two individuals who went hunting on property belonging to an Army depot where both were employed.[58] This hunting was permitted, provided 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

---

[52] Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 90 Iowa L. Rev. 553, 583 (1995).

[53] 5 U.S.C. § 552a(b).

[54] 5 U.S.C. §552a(4).

[55] Houston v. United States Dept. of Treasury, 494 F.Supp. 24, 27-28 (D.D.C. 1979).

[56] A nice comparison of the federal and state language appears here: http://www.oag.state.tx.us/notice/privacy_table.htm (visited March 22, 2010).

[57] Quinn v. Stone, 978 F.2d 126 (3d. Cir. 1993).

[58] *Id*. at 128-29.

investigation, the officer examined the hunting registry and also obtained one of the plaintiff's time cards to investigate a (false) claim that she had purported to be at work on the day she was hunting.[59] 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.

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." One of the plaintiffs had listed his address and phone number in the local telephone directory. The court, remarkably, 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." 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.][60]

In short, the court says, 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 in the phone book and gotten his phone number and address, there would be no Privacy Act violation if the Army subsequently disclosed that information to the investigator. But because the Army's disclosure happened first, the Act was violated.

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 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.[61]

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 already readily accessible to the public. One wants to deter the government from disclosing information where such disclosure is

[59] *Id*. at 130.
[60] *Id*. at 134.
[61] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. Chi. L. Rev. 919, 935 (2005).

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 *Reporter's Committee*—the government should not be permitted to disclose "practically obscure" information about an individual—the case against such disclosure simply 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*,[62] 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.[63] 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. 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."[64] 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.[65]

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, 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 *Reporter's 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

[62] 73 F.3d 1111 (D.C. Cir. 1996).
[63] *Id*. at 1117-24.
[64] *Id.* at 1112.
[65] *Id*. at 1123 n. 10.

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.[66]

Now we see the potential difficulties. The government might intentionally release a record containing exclusively 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. What is to be done?

Doe v. Chao is the Supreme Court's most significant decision concerning the Privacy Act.[67] In *Chao* the Court had to construe the 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, and the Department then used the Social Security Number 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 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. 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 six-to-three 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. Along the way, the Court held that subsection (a)'s reference to a "person entitled to recovery" meant someone who had sustained "actual damages." The clear implication of the Court's analysis is that if Doe had prudently 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 zilch. That seems odd. Two very interesting passages from Justice Souter's majority opinion try to parry this concern:

[66] 5 U.S.C. §552a(g)(4)(A)
[67] 540 U.S. 614 (2004).

> 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 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.[68]

Fascinating stuff. The Court is telling us that tort principles are going to help it interpret the Privacy Act's ambiguous minimum statutory damages language. Yes, the hypothetical Doe who signs up for identity theft protection 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" where 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* made several compelling statutory interpretation arguments. As she points 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."[69] The dissent is quite effective in pointing out that similar language in other federal statutes had been construed to permit recovery of minimum damages without a showing of pecuniary harm.[70] There were 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.[71] 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.[72] No academics doing work in the area submitted amicus briefs in support of the Labor

[68] *Chao*, 540 U.S. at 621-25.

[69] *Id*. at 631 (Ginsburg, J., dissenting).

[70] *Id*. at 639-41.

[71] *See supra* text accompanying note 66.

[72] *See* Brief of Amici Curiae Electronic Privacy Information Center . . . and 16 Legal Scholars and Technical Experts in Support of Petitioner, Doe v. Chao (Aug. 25, 2003), available at 2003 WL 22070504. That was the only amicus brief the author has ever signed, and the author has now learned his lesson.

Department's interpretation. The majority's statutory interpretive 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 that I understand what the majority might have been trying to do. We can understand *Doe* as another exemplary "re-unifying 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 v. Stone* 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. *Doe v. Chao*, in short, is the second wrong that made a right.

So far, *Doe v. 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.[73] 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 defamation principles may prove decisive in helping judges decipher the meaning of ambiguous terms, certainly privacy tort principles must be all the more helpful. Yet *Quinn* and *Pilon* aren't just out of step with privacy tort principles—they are in a completely different galaxy.[74] Properly understood, *Doe v. Chao* points toward the radical revision of Privacy Act jurisprudence. But no one seems to have noticed.

V.

To say that privacy law should be reunified along the lines described by Warren and Brandeis is not to suggest that they gave us in 1890 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 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

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

[74] 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 54. 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 11-year old criminal conviction may be tortious), *with* Gates v. Discovery Communications, Inc., 101 P.3d 552 (Cal. 2004) (holding that *Briscoe* must be overruled in light of subsequent U.S. Supreme Court precedents).

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 (i.e., were highly offensive to a reasonable person).[75] We should add to this inquiry the basically welfarist balancing test that Warren and Brandeis embraced in 1890 and that Judge Posner snuck 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 reputational harms compound dignitary harms, and the reputational harms in a pure intrusion case are necessary 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.[76]

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 tried to bring 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. That 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.[77]

Returning privacy tort law to the 1890's era status quo is attractive, and it does not require the replacement of Prosser's framework with element-less torts. We can embrace a

---

[75] The intuition here is that social norms relating to information privacy will tend to be social welfare maximizing. *See* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); Strahilevitz, *supra* note 61, at 925-31, 983.

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

[77] For example, the Supreme Court has left the elements of a state law intentional infliction of emotional distress cause of action but held separately that in cases involving a public figure plaintiff, the First Amendment requires the plaintiff to demonstrate actual malice in order to recover. *See* Hustler Magazine v. Fallwell, 485 U.S. 46, 56 (1988).

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 highly offensive to a reasonable person, and (3) engages in conduct that engenders social harms that exceed the associated social benefits.

Having achieved the perfect fix for all the problems with privacy tort law,[78] 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 paper has already shown how the Privacy Act and Freedom of Information Act 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.[79]

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 web sites, or location-aware smartphones. But there have been many opportunities presented for judges to address these problems via tort rules. In some cases, such as data broker sales of information that might compromise an individual's safety, the courts have been willing to expand tort liability to regulate dangerous conduct.[80] But in the majority of cases, the courts have understood themselves to be junior partners to legislators in dealing with new privacy challenges.[81] 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.

There is no good reason why the great privacy innovations of the twentieth century—like the Fair Information Practices—cannot be incorporated into privacy tort law at the remedial stage. 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, to provide opportunities for data privacy subjects to correct errors in those dossiers when they can show that such information is indeed erroneous, to obtain the subject's informed consent when sensitive data is transferred to another entity for another purpose, and to 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

[78] I'm kidding.

[79] 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 (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 Communications Technologies: A Call to the Rescue of the Attorney-Client Privilege*, 39 How. L.J. 437, 450 (1996).

[80] Remsburg v. Docusearch, 816 A.2d 1001 (N.H. 2003).

[81] Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. 1995); Shibley v. Time, 341 N.E.2d 337 (Ohio Ct. App. 1975).

law. 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.

VI.

I have argued that coherence in privacy law is basically achievable. The question remains whether such coherence is normatively desirable.[82] The answer is yes, for at least three reasons.

First, coherent law lowers the compliance costs for individuals and organizations. Just as firms doing business in a number of markets typically will prefer that the laws of various jurisdictions be harmonized, they will 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 the common law torts and European Union privacy directives. Government lawyers may need to familiarize themselves with each of these statutory frameworks, plus the Privacy Act, Freedom of Information Act, and the constitutional right of information privacy. Safeguarding privacy interests is most cost effective when this alphabet soup of provisions do not conflict with one another, and when knowledge about one privacy system can be leveraged to help understand another.

The world in which post-Prosser privacy lawyers find themselves is one of enormous and needless complexity. 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, to say nothing of laymen.[83]

Second, the complexity and fragmentation of privacy law limits the gains available in common law adjudication. When courts treat Privacy Act law or FOIA privacy or privacy tort law as a walled garden they require that wheels be reinvented, and 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

[82] There is, of course, a voluminous legal literature on coherence – and I do not purport to make any theoretical contributions to that longstanding debate here. *See generally* RONALD DWORKIN, LAW'S EMPIRE 176-275 (1986); Joseph Raz, *The Relevance of Coherence*, 72 B.U. L. Rev. 273 (1992); Cass R. Sunstein et al., *Predictably Incoherent Judgments*, 54 Stan. L. Rev. 1153 (2002).

[83] *See generally* Dworkin, *supra* note 82, at 188 ("If people accept that they are governed not only by explicit rules laid down in past political decisions but by whatever other standards flow from the principles these decisions assume, then the set of recognized public standards can expand and contract organically, as people become more sophisticated in sensing and exploring what these principles require in new circumstances, without the need for detailed legislation or adjudication on each possible point of conflict.").

Of course we need not embrace Dworkin's Herculean task of engendering the coherence of privacy law with all other bodies of substantive law. Rather, we should be willing to settle for information privacy law's internal consistency, recognizing it as an appropriately compartmentalized field. *See id*. at 250-53 (discussing local priority); *see also* Sunstein et al., *supra* note 82, at 1200-01 (discussing the value of "local coherence" in a compartmentalized body of law).

that will arise later in tort cases, 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 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. The Freedom of Information Act says yes, such that the government can withhold the addresses of federal workers.[84] Privacy tort law says no, such that there is no civil liability for disclosing the home address of an individual.[85] 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.[86] 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.[87] Once again, this sort of incoherence goes unrecognized whenever we excuse privacy law's fragmentation.[88]

Third, the fragmentation of information privacy law means that similarly situated individuals are treated differently. Coherence lends itself to equal treatment as a general matter,[89] and that principle is equally valid in privacy law's domain. The relatives of a deceased individual should have the same rights to prevent the publication of autopsy photographs regardless of whether those photographs are possessed by a private actor or public actor—the harms to dignitary interests resulting from publication will be the same in either case. But the law seemingly gives the next of kin more privacy protection in those instances where the federal government possesses the photographs, less privacy protection where a private actor possesses those photographs, and no privacy protection where the state improperly releases those photographs to a private actor, who publishes them.[90] Reunifying privacy law would, at the very least, remedy the first of these inconsistencies.

VII.

On March 8, 2010, the Supreme Court granted certiorari in *Nelson v. NASA*. To privacy scholars, this was a stunning turn of events. It has been thirty-three years since the Supreme Court 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 presented on appeal. In granting cert, the court accepted an invitation by Chief Judge Kozinski, whose dissent from the denial of a rehearing en banc ended as follows:

---

[84] United States Department of Defense v. Federal Labor Relations Authority, 510 U.S. 487, 502 (1994).

[85] Johnson v. Sawyer, 47 F.3d 716, 732-33 (5th Cir. 1995) (en banc).

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

[87] Paul P. v. Verniero, 170 F.3d 396, 403-04 (3rd Cir. 1999).

[88] 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. *Id.* at 404.

[89] Dworkin, *supra* note 82, at 222.

[90] *See generally* text accompanying notes 37-41 and Florida Star v. B.J.F., 491 U.S. 524 (1989).

> [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.[91]

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 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.

Nelson involves the federal government's use of detailed background checks to investigate the suitability of Jet Propulsion Laboratory (JPL) employees for continued employees. 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."[92] 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, whether they had used abusive language, been involved in personality conflicts, developed mental, emotional, psychological, or psychiatric issues, or engaged in sodomy. In addition, third parties were to 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.[93] 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.[94]

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."[95] While the court held that the government's inquiries into its employees' backgrounds was legitimate, it applied intermediate scrutiny and held that the government's investigations were

---

[91] Nelson v. NASA, 568 F.3d 1028, 1054 (9th Cir.) (Kozinski, C.J., dissenting from the denial of rehearing en banc).

[92] *Nelson*, 568 F.3d at 1029 n.3 (Wardlaw, J., concurring in the denial of rehearing en banc).

[93] *Id*. at 1032-33.

[94] *Id*. at 1033.

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

not narrowly tailored to further those interests.[96] The court of appeals repeatedly 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.

As the judges debated whether to consider the case en banc, several disagreements emerged. The most important for our purposes 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.[97]

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 of information privacy case. As they saw it, "the 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."[98]

The back and forth between Judges Callahan and Wardlaw is deeply unsatisfying. Callahan is saying privacy law should be unified because the Ninth Circuit shouldn't do something inconsistent with what the Supreme Court has done. Wardlaw's response is essentially a bare assertion: "no it shouldn't." Whereas this paper is obviously sympathetic to Callahan's methodology, her execution 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 that in a case involving overlap between the Fourth Amendment and the

[96] *Nelson*, 568 F.3d at 1032.
[97] *Id* at 1044 (Callahan, J., dissenting from the denial of rehearing en banc) (citations omitted).
[98] *Id*. at 1031 n 7 (Wardlaw, J., concurring in the denial of rehearing en banc).

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 rights.

Having said that, 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 the courts have held that such inquiries do not amount to an intrusion upon seclusion. The leading American case on this point is *Nader v. General Motors*, a New York Court of Appeals case in which the court held that General Motors' very intrusive interviews of Ralph Nader's associates and friends were not an intrusion upon seclusion.[99] 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 tort law has by-and-large rejected *Nader*'s "third party doctrine" approach to tort law.[100] As it happens, California is the rare American jurisdiction where privacy tort law and constitutional privacy law have mostly merged—thanks to the California Constitution's privacy clause, which lacks a state action requirement.[101] As a result, many privacy cases that could be brought under a tort theory are brought under the state constitution. Some of those state constitutional cases 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.[102] Another 1991 case holds 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 state Constitution.[103] But 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 reserve judgment on how its ruling should apply to workplace settings.[104] Moreover, the state courts have rejected one of the central rhetorical arguments put forward by the *Nelson* court, which was that employees have much stronger privacy protections than mere job seekers.[105] It is strange that in California the state 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. There is a good chance that the plaintiffs in *Nelson* could have prevailed had they pursued a state tort or constitutional claim.

---

[99] 255 N.E.2d 765 (N.Y. 1970).

[100] For a lengthier discussion of the case law, see Strahilevitz, *supra* note 61, at 939-46.

[101] 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 and pursuing and obtaining safety, happiness, and privacy."); Soroka v. Dayton Hudson Corp., 18 Cal.App.4th 1200, 1210 (Cal. Ct. App. 1991).

[102] Long Beach City Employees Ass'n v. City of Long Bach, 719 P.2d 660, 670 (Cal. 1986).

[103] *Soroka*, 18 Cal.App.4th at 1214.

[104] Hill v. NCAA, 865 P.2d 633, 664 (Cal. 1994).

[105] *Id*. at 1210.

Under the applicable state tort law, sharing information with friends and associates does not necessarily waive reasonable expectations of privacy against the information being shared with outsiders. Under state constitutional law, employers are likely prohibited from asking questions about lawful sexual practices, and perhaps about drug treatment as well, though it is worth noting that the Supreme Court's grant of certiorari evidently encompassed the drug treatment inquiry but not questions about sodomy.[106] Moreover, NASA employees could sue the federal government under a tort theory, given the sovereign immunity waiver in the Federal Tort Claims Act. In these circumstances, the availability of a federal constitutional cause of action represents a belt-and-suspenders approach.

The Supreme Court may well decide in *Nelson* that there is no such thing as a constitutional right of 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. The Court will no doubt be tempted to follow the Sixth Circuit's approach, which has significant appeal. Such an approach would view the sorts of harms to privacy interests that arose in *Nelson* as ordinary tort harms that are appropriately pursued through garden-variety tort causes of action. The primary appeal of this approach is one of error-correction: If the judges make a mistake in deciding difficult, subjective questions of privacy law, those errors can be fixed via ordinary legislation at the state or federal level rather than via the cumbersome, lengthy, and difficult processes of amending the federal Constitution or changing the composition of the Court through appointments.

Having said that, the approach of killing off the constitutional right of information privacy creates two distinct problems. First is what we can call the Bobby Ewing dilemma. *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. Fans of the show were displeased—Bobby's shower may well have been the moment at which what was once TV's most popular show definitively lost its luster.

In its two 1977 cases, the U.S. Supreme Court devoted pages and pages of the U.S. Reports to discussing the constitutional right of 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 developing 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 public in general know little about.

Second, there is a perhaps small category of cases that fall through the cracks of existing privacy protections where the wrong by the state to the individual is egregious. The challenge is in finding them. Many of the landmark constitutional right of information privacy cases are like *Nelson* in that they could have been brought under a state tort or state constitutional theory. One

[106] The government's petition for certiorari sought review of the Ninth Circuit's ruling only with respect to previous drug treatment and open ended questions about whether the person being interviewed had other adverse information about the subject of the background investigation. See NASA v. Nelson, Petition for a Writ of Certiorari 1 (U.S. Nov. 2, 2009), available at 2009 WL 3614469.

prominent example would be a case like *Doe v. Borough of Barrington*.[107] An arrestee with bleeding lesions discloses his HIV positive status to police officers taking him into custody so that they take appropriate precautions to protect themselves from infection, and a member of the same police department subsequently informs the arrestee's neighbors of his HIV status. A panic ensues, causing various neighbors to pull nineteen children out of the public school attended by the arrestees' children for fear of them contracting the disease through casual conduct. A media report on the panic then disclosed the Does' real names.[108]

The court understandably ruled in *Doe*'s favor, and *Doe* is included as a principal constitutional right to information privacy case in Solove and Schwartz's leading privacy law casebook.[109] But Doe did bring pendent state tort invasion of privacy claims under New Jersey law,[110] and those claims would have fared well under state law. New Jersey is a state where the state tort claims act permits causes of action for invasion of privacy to be asserted.[111] And New Jersey, along with most states, recognizes the tort for public disclosure of private facts.[112] The primary differences between the federal constitutional claim and the state tort claim are twofold: the former created a basis for federal jurisdiction, and enabled the plaintiffs to more easily recover attorneys' fees if successful. There is thus a "gap" in New Jersey privacy law, but it is more strategic than substantive. On the one hand, one might compare the facts of *Barrington* to the facts of garden-variety civil rights suits and say that Doe ought to be as entitled to attorneys' fees as the litigants in those cases. But on the other hand, the question of attorneys' fees and a federal forum seems like the sort of question best addressed through ordinary legislation rather than constitutional interpretation. The gap is much wider in a jurisdiction like North Carolina, which prohibits invasion of privacy tort suits against the states and which lacks a California-style state constitutional provision to permit tort-like claims to proceed in the state courts.[113] If we place the facts of *Barrington* in Charlotte, North Carolina, then, the question of whether there will be a constitutional right to information privacy boils down to the question of whether there ought to be any remedy at all for that disturbing governmental conduct.

The basic question presented in *Nelson*, then, is whom and what should fill these gaps—be they small (as in New Jersey) or large (as in North Carolina). The *Nelson* panel thought that the federal courts and federal Constitution should fill them, whereas Judge Callahan's dissent, implicitly argued that these gaps be addressed to the state courts and state legislatures. Superficially, either approach can be squared with an attempt to reunify privacy law. A more persuasive version of the panel 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. We would just be replacing incoherence with reified inconsistency.[114]

---

[107] 729 F. Supp. 376 (D.N.J. 1990).
[108] *Id*. at 379.
[109] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 479 (3d ed. 2009).
[110] *Id*. at 379.
[111] Leang v. Jersey City Bd. Of Educ., 969 A.2d 1067, 1107, 1115-17 (N.J. 2009).
[112] Romaine v. Kallinger, 537 A.2d 284, 297 (N.J. 1988).
[113] *See supra* note 23.
[114] 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 the other circuits, which do.

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 do are blunted. Judge Callahan's approach would create coherence by withdrawing the federal Constitution from the domain of information privacy protections—leaving 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 of 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 or jurisdictions where state law remedies are unavailable for serious wrongs.[115] 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 state employees exceed the national security benefits? Affirmative answers to all three questions would suggest that the constitutional right to information privacy has been violated, reunifying the law of privacy by creating national uniformity.

Readers with comments may address them to:
Professor Lior Strahilevitz
University of Chicago Law School
1111 East 60th Street
Chicago, IL 60637
lior@uchicago.edu

[115] To be clear, as a matter of substantive law, I strongly favor the waiver of sovereign immunity for invasion of privacy suits against the states. But if a jurisdiction unwisely chooses not to waive sovereign immunity, it is not obvious that the Constitution should nevertheless compel liability.

The University of Chicago Law School
Public Law and Legal Theory Working Paper Series

For a listing of papers 1–250 please go to http://www.law.uchicago.edu/publications/papers/publiclaw

251. Tom Ginsburg, The Clash of Commitments at the International Criminal Court (November 2008)
252. Tom Ginsburg, Constitutional Afterlife: The Continuing Impact of Thailand's Post-Political Constitution (November 2008)
253. Cass R. Sunstein and Richard Zechkauser, Overreaction to Fearsome Risks (December 2008)
254. Gilbert Metcalf and David Weisbach, The Design of a Carbon Tax (January 2009)
255. David Weisbach, Responsibility for Climate Change, by the Numbers (January 2009)
256. Daniel Abebe, Great Power Politics and the Structure of Foreign Relations Law (January 2009)
257. Brian Leiter, Moral Skepticizm and Moral Disagreement in Nietzsche (January 2009)
258. Adam B. Cox, Immigration Law's Organizing Principles, (February 2009)
259. Adam Samaha, Gun Control after *Heller*: Threats and Sideshows from a Social Welfare Perspective (February 2009)
260. Lior Strahilevitz, The Right to Abandon (February 2009)
261. Lee Fennell, Commons, Anticommons, Semicommons (February 2009)
262. Adam B. Cox and Cristina M. Rodríguez, The President and Immigration Law (March 2009)
263. Mary Anne Case, A Few Words in Favor of Cultivating an Incest Taboo in the Workplace (April 2009)
264. Adam B. Cox and Eric A. Posner, The Rights of Migrants (April 2009)
265. John Bronsteen, Christopher J. Buccafucso, and Jonathan S. Masur, Welfare as Happiness (June 2009)
266. Mary Anne Case, No Male or Female, but All Are One (June 2009)
267. Bernard E. Harcourt, Alon Harel, Ken Levy, Michael M. O'Hear, and Alice Ristroph, Randomization in Criminal Justice: A Criminal Law Conversation (June 2009)
268. Bernard E. Harcourt, Neoliberal Penality: A Brief Genealogy (June 2009)
269. Lee Anne Fennell, Willpower and Legal Policy (June 2009)
270. Brian Leiter, Nietzsche's Philosophy of Action, July 2009
271. David A. Strauss, The Modernizing Mission of Judicial Review, July 2009
272. Lee Anne Fennell and Julie Roin, Controlling Residential Stakes, July 2009
273. Adam M. Samaha, Randomization in Adjudication, July 2009
274. Jonathan Masur and Eric A. Posner, Against Feasibility Analysis, August 2009
275. Brian Leiter, Foundations of Religious Liberty: Toleration or Respect?, October 2009
276. Eric A. Posner and Adrian Vermeule, Tyrannophobia, September 2009
277. Bernard E. Harcourt, Henry Louis Gates and Racial Profiling: What's the Problem? September 2009
278. Lee Anne Fennell, The Unbounded Home, Property Values beyond Property Lines, August 2009
279. Brian Leiter, The Epistemic Status of the Human Sciences: Critical Reflections on Foucault, October 2009
280. Ward Farnsworth, Dustin F. Guzior, and Anup Malani, Ambiguity about Ambiguity: An Empirical Inquiry into Legal Interpretation, October 2009
281. Anup Malani, Oliver Bemborn and Mark van der Laan, Accounting for Differences among Patients in the FDA Approval Process, October 2009
282. Saul Levmore, Ambiguous Statutes, November 2009
283. Rosalind Dixon, Female Justices, Feminism and the Politics of Judicial Appointment: A Reexamination, November 2009

284. Rosalind Dixon, The Supreme Court of Canada, *Charter* Dialogue and Deference, November 2009
285. Rosalind Dixon, A Minimalist Charter of Rights for Australia: The U.K. or Canada as a Model? November 2009
286. F. Scott Kieff and Richard A. Epstein, Supreme Court Brief of Dr. Ananda Chakrabarty as Amicus Curiae in Support of Petitioners in Bilski (December 2009)
287. Jacob E. Gersen and Anne Joseph O'Connell, Hiding in Plain Sight? Timing and Transparency in the Administrative State (December 2009)
288. Richard A. Epstein, Impermissible Ratemaking in Health-Insurance Reform: Why the Reid Bill Is Unconstitutional (December 2009)
289. Brian Leiter, Why Legal Positivism? (December 2009)
290. Anu Bradford and Eric A. Posner, Universal Exceptionalism in Internatinal Law (February 2010)
291. Daniel Abebe and Eric A. Posner, Foreign Affairs Legalism: A Critique (February 2010)
292. Tom Ginsburg, Eastphalia as a Return to Westphalia (February 2010)
293. Tom Ginsburg, Lawrence Friedman's Comparative Law (February 2010)
294. Tom Ginsburg, Studying Japanese Law because It's There (February 2010)
295. Tom Ginsburg, Judicial Indipendence in East Asia: Implications for China (February 2010)
296. Tom R. Tyler, Stephen Schulhofer, and Aziz Huq, Legitimacy and Deterrence Effects in Counter-Terrorism Policiing: A Study of Muslim Americans (February 2010)
297. Alison L. LaCroix, Federalists, Federalism, and Federal Jurisdiction (February 2010)
298. Brian Leiter, Rorty and the Philophical Tradition: A Comment on Professor Szubka (March 2010)
299. Aziz Z. Huq, Against National Security Exceptionalism (March 2010)
300. Anu Bradford, When the WTO Works, and How It Fails (March 2010)
301. Aziz Z. Huq, Modeling Terrorist Radicalization (March 2010)
302. Adam M. Samaha, On Law's Tiebreakers (March 2010)
303. Brian Leiter, The Radicalism of Legal Positivism (March 2010)
304. Lee Anne Fennell, Unbundling Risk (April 2010)
305. Aziz Z. Huq, What Good Is Habeas? (April 2010)
306. Aziz Z. Huq, Easterbrook on Academic Freedom (April 2010)
307. Jonathan S. Masur and Jonathan Remy Nash, The Institutional Dynamics of Transition Relief (April 2010)
308. Alison L. LaCroix, Temporal Imperialism (May 2010)
309. Lior J. Strahilevitz, Reunifying Privacy Law (May 2010)