REWORKING INFORMATION PRIVACY LAW

A Memorandum Regarding Future ALI Projects About Information Privacy Law

Paul M. Schwartz
Professor of Law
U.C. Berkeley School of Law

Daniel J. Solove
John Marshall Harlan Research Professor of Law
George Washington University Law School

August 2012

TABLE OF CONTENTS

I. INTRODUCTION: PRIVACY LAW AND ALI PROJECTS

Privacy law in the United States is currently a bewildering assortment of many types of law that differ from state to state and that are also found in the federal code. It is unwieldy, conflicting, and overwhelming. Significant work must be done to bring this enormous body of law into some semblance of order.

US law is largely a bottom-up approach. It has emerged as a reaction to specific problems. It has many sources, works in so many different ways, and, as a result, lacks the coherence of a more abstract and top-down approach. The law in the US is a cacophony of so many different laws and cases that it often lacks consistency or definitive answers.

Due to the condition of US law, many foreign nations discount the protections that US law does have. The European Union (EU), for example, has doubts about the level of protection in US privacy law, and its view is creating significant tensions and problems for smooth transborder data flows and efficient commerce between EU members and the US. The latest manifestations of these difficulties occur in the debate about the EU's Draft Data Protection Regulation (2012) and about cloud computing. The Draft Data Protection Regulation contains measures that are likely to make data exports to the US more difficult, including heightened powers for EU regulators. In cloud computing, specialized companies deliver software, infrastructure, and storage over the Internet. Some EU Member Nations are skeptical of clouds that US companies manage. Their perception is that the US government will easily gain access to the personal information of citizens of EU Member Nations stored in such environments.

Many in the EU may be looking for simple and clear articulations of principles in US privacy law. When they only find scant bright lines and few crisp rules, it may prove easy for them to dismiss US law as inadequate. In fact, when the totality of federal and state statutes, constitutional provisions, and common law protections are considered, there can be quite a lot of protection under certain circumstances in the US. Of course, there are all sorts of idiosyncratic

cracks and crevices in US privacy law, but there are many instances where the US has more stringent privacy protection than the EU.

Thus, privacy law calls out for the kind of guidance that the ALI can bring. In this Memorandum, we have identified multiple, important projects where the ALI can help bring greater order and consistency to privacy law and provide guidance to courts and legislatures.

At this juncture, it will be helpful to discuss the types of projects that the ALI sponsors. These are Restatements of Law, Model Statutes, and Principles of Law. An understanding of these existing models will be helpful in assessing potential privacy projects for the ALI.

Restatements of Law

The best known of the ALI's projects are its Restatements of areas of the common law. As Lance Liebman has explained, "A Restatement is a positive statement of legal doctrine on a legal subject on which American law is made by common law judges rather than by elected legislatures or administrative agencies."[1] Before World War II, the ALI had already published Restatements of Contracts, Agency, Conflict of Laws, Trusts, Restitution, Torts, Security, Judgments, and Property. Among the post-War Restatements is the Restatement (Second) of Torts, which contains the most influential expression of the modern privacy torts.

Current ALI projects in this category include the Restatement (Third) of Torts, Liability for Physical and Emotional Harm; Restatement (Third) of Torts, Liability for Economic Harm; Restatement (Third), the U.S. Law of International Commercial Arbitration; Restatement (Third), The Law of Consumer Contracts; Restatement (Third) Employment Law; Restatement (Third), Restitution and Unjust Enrichment.

[1] Lance Liebman, *The American Law Institute: A Model for the New Europe?* 5 (ms., 2012).

Model Statutes

The ALI has also published significant Model Statutes, including the Model Penal Code, the Uniform Commercial Code (UCC), and proposed federal income tax statutes. As Liebman has stated of these efforts, which began post-World War II, they are "forward-looking efforts that could influence federal and state legislatures as well as courts."[2] The UCC marked a collaboration between the ALI and the National Conference of Commissioners on Uniform State Laws.

Current ALI projects of this type include the Model Penal Code: Sentencing.

Principles of Law

The ALI does more than sponsor work that restates common law doctrine or creates draft statutes. Its Principles of Law constitute analysis of issues that are directed towards courts, legislative bodies, and governmental agencies. The first Principle of Law was carried out on the topic of Corporate Governance, which was followed by one on Principles of Law of Family Dissolution.

Current ALI projects of this type include Principles of the Law of Nonprofit Organizations; Principles of Government Ethics; Principles of the Law of Liability Insurance; and Principles of Election Law: Resolution of Election Disputes.

Transnational Projects

The ALI's portfolio of projects also includes transnational work. The form of this work can take the form of a Principle of Law, which we have just discussed. The first such effort was the creation of Guidelines Applicable to Court-to-Court Communications in Transborder Cases. Another important venture was Principles of Transnational Civil Procedure.

[2] Id. at 9.

Current ALI projects of this type are Principles of World Trade. In addition, there is a project on Transnational Insolvency: Principles of Cooperation.

With this typology of different kinds of ALI projects established, we now wish to discuss possible areas for ALI work in the privacy area. These projects fall into areas involving public law, private law, and mixed areas. As an overview, we provide the following list:

PRIVATE LAW PROJECTS

- Rethinking the Privacy Torts
- Negligence, Strict Liability, and Duties Owed Regarding the Use and Disclosure of Personal Data
- Guiding Principles of Privacy Law
- Data Security Breach Notification
- Beyond Notice and Choice
- Harmonization with International Law

PUBLIC LAW PROJECTS

- Privacy and Free Speech
- Intellectual Privacy and Anonymity

MIXED PRIVATE LAW/PUBLIC LAW PROJECTS

- Defining PII
- Systematic Data Access: Data Mining and Beyond
- Drones
- Defining Privacy Harms
- Education Privacy

II. PRIVATE LAW PROJECTS

A. Rethinking the Privacy Torts

In 1890, Samuel Warren and Louis Brandeis published a seminal article, *The Right to Privacy.* In it, they called for tort law to develop remedies to protect privacy.[3] The law then heeded their call for reform. As early as 1903, courts and legislature responded to the Warren and Brandeis article by creating a number of privacy torts to redress the harm that the two authors had noted.

In 1960, in an article entitled *Privacy*, William Prosser reformulated the series of cases spawned by the Warren and Brandeis article. Prosser created a taxonomy for the more than three hundred cases decided in the seventy years since the Warren and Brandeis article. For Prosser, the "law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff ... ." The four Prosser privacy torts are:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[4]

Under the leadership of Prosser, who was a reporter for the Restatement (Second) of Torts, these four proposed torts became part of the Restatement.[5]

This section of the Restatement had a profound effect on the law. Today, the vast majority of jurisdictions recognize the privacy torts, and they nearly all use the Restatement's version of the torts. The formulations in the Restatement (Second) of Torts are:

• *Intrusion Upon Seclusion*: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[4] William Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960).
[5] Restatement (Second) of Torts § 46 (1977).

liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[6]

• *Public Disclosure of Private Facts:* "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[7]

• *False Light*: "One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[8]

• *Appropriation of Name or Likeness*: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[9]

Many have criticized the torts for not adequately protecting privacy. Already in 1983, Diane Zimmerman titled her article on the Warren & Brandeis privacy torts, "Requiem for a Heavyweight."[10] Switching metaphors from boxing to the maritime, Zimmerman wondered, "Is it possible that the seemingly elegant vessel that Warren and Brandeis set afloat some nine decades ago is in fact a leaky ship which should at long last be scuttled?"[11]

[6] Restatement (Second) of Torts § 652B (1977).
[7] Restatement (Second) of Torts § 652D (1977).
[8] Restatement (Second) of Torts § 652E (1977).
[9] Restatement (Second) of Torts § 652C (1977).
[10] Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 Cornell L. Rev. 291 (1983).
[11] Id. at 294.

Prosser has not fared much better than Warren & Brandeis in the evaluation of many scholars. A symposium in the California Law Review in 2010, which marked the fiftieth anniversary of Prosser's *Privacy* article, featured far more criticisms than praise of the four privacy torts.

What are the weaknesses of the privacy torts? As we will now discuss, these start with a narrow concept of privacy, which lacks nuance and fails to acknowledge many circumstances in which people expect privacy. There is also an exception in the privacy torts for newsworthy matters, which judges often apply in a fashion that is highly deferential to the media. As a related matter, the torts of public disclosure of private facts and intrusion upon seclusion only protect against acts that are "highly offensive to a reasonable person." The contemporary impact of blogs and other media devoted to gossip may have raised this standard to a troubling level that is quite difficult to reach.

Other weaknesses of the privacy torts concern the separate status of the related torts of the intentional infliction of emotional distress and breach of confidentiality. Both torts are clearly related to the privacy torts, and the ALI might consider an integrated treatment of them. Similar integration is needed of the "right of publicity" tort, which is an offshoot of the tort of appropriation. The Restatement currently includes only the appropriation tort, however, and that tort has important conceptual differences with the publicity interest.

There are also a host of modern areas of information processing in which the privacy torts prove of little assistance. These include the issues of "Big Data," data security, and privacy policies. Overall, the goal of any assessment of the privacy torts should be to find a way to reignite their development.

1. A Narrow Conception of Privacy

Courts have adopted a very narrow concept of privacy, which limits the privacy torts. Many courts see privacy as tantamount to total secrecy, and fail to recognize any privacy interests in behavior in the public, when information is in the public domain, or when

information is known by others. This narrow conception of privacy lacks nuance and fails to understand that people sometimes do expect privacy in such circumstances. For example, people might expect privacy in places open to the public, such as a gym locker room, or for a conversation in a restaurant that they take reasonable efforts to shield from being overheard.

People also expect "privacy by obscurity," that is, the ability to blend into a crowd or find other ways to be anonymous by default. This condition is rapidly disappearing, however, with new technologies that can capture images and audio nearly everywhere. As an example, facial recognition technology is constantly improving. Already, Facebook and Apple use technologies that permit the automatic tagging of photographs.[12] One day devices, such as Google Glasses, may permit the identification of passing pedestrians on the street.[13] In short, if the privacy torts are to be rethought, more guidance must be provided as to the underlying concept of privacy.

We also now have an opportune time to provide guidance about how to understand privacy in a more nuanced way. Recently, in *United States v. Jones*, the Supreme Court held that the Government's installation and use of a GPS device on a suspect's vehicle constitutes a "search" subjecting it to Fourth Amendment scrutiny.[14] Notably, this activity occurred in public. The reasoning of five justices in concurring opinions noted that extensive surveillance in public could implicate a reasonable expectation of privacy.[15] Prior to this time, a majority of justices on the Court had viewed privacy as akin to total secrecy and did not recognize any privacy in public.

---

[12] Justin Mitchell, Making Photo Tagging Easier, The Facebook Blog, December 15, 2010 (updated June 7, 2011 and June 30, 2011), http://www.facebook.com/blog/blog.php?post=467145887130; David Goldman, Real-time face recognition comes to your iPhone camera, CNN Money, March 12, 2012, http://money.cnn.com/2012/03/12/technology/iPhone-face-recognition/index.htm.

[13] See Nick Bilton, Behind the Google Goggles, Virtual Reality, The New York Times, February 22, 2012, www.nytimes.com/2012/02/23/technology/google-glasses-will-be-powered-by-android.html?_r=3.

[14] U.S. v. Jones, 132 S. Ct. 945, 949 (2012).

[15] See id at 957 ("I would not assume that all information voluntarily disclosed to some member of the public … is, for that reason alone, disentitled to Fourth Amendment protection.")(Sotomayor, J., concurring); id at 964 ("Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.") (Alito, Ginsburg, Breyer, & Kagan, JJ., concurring).

If the Supreme Court recognizes a new direction in its Fourth Amendment privacy jurisprudence, the torts might also move in a related direction. This result might follow because Fourth Amendment case law has exercised a significant influence on the tort cases. Courts in these cases draw on the Supreme Court's concept of reasonable expectations of privacy in defining the privacy elements of the torts. When no reasonable expectation of privacy can be found concerning the underlying activity, the intrusion or private fact, a judge will frequently be reluctant to find a violation of a privacy tort.

But many questions remain about how such a new concept of privacy should apply. Certainly, merely being observed in public or subject to some surveillance on one occasion in public should not trigger a privacy violation. When does surveillance in public become extensive enough to trigger a reasonable expectation of privacy? How much is too much? Will a broader view of privacy be workable?

2. The Tests of Newsworthiness and "Highly Offensive"

The public disclosure of private facts tort is limited by the newsworthiness test. This approach looks to whether a matter is of "legitimate public concern." If it is, then the tort is inapplicable. The newsworthiness test balances privacy and free speech interests.

Courts have used numerous tests for newsworthiness; there is little consensus on this issue. Yet, a shared trend has been the great deference of many courts to the media. These courts let the publisher rather than the judiciary decide the proper subject for news. The result is that it becomes more or less impossible for any plaintiff to prevail.

What should the standard be? If courts do not evaluate the judgment of the press, will everything be per se newsworthy once it is published? But do we want courts and juries second-guessing the decisions of journalists?

There is another problem with a test that defers to the media. In today's age of blogs and social media, the definition of "media" has become quite fuzzy. Anyone with a blog or a website

that hosts content might be considered to be the publisher of media. The Restatement (Second) of Torts suggests that courts are to decide newsworthiness by looking at the "customs and conventions of the community."[16] Yet, at present, there may be neither a stable profession of "journalism" nor stable norms of professional behavior for journalists. As a consequence, deference to the "media" might simply mean letting anyone with a website decide what is of "legitimate public concern," and, hence, unprotected by the private facts tort.[17]

As a final matter, it seems today that nearly any piece of gossip will become fodder for the news. Yet, the private facts tort only protects matters that, if publicized, "would be highly offensive to a reasonable person." The torts of intrusion upon seclusion and false light contain a similar limitation. It may be that gossip blogs and other online fora have reduced the ability of the law to find publicity "highly offensive." In a comment to the private facts tort, the Restatement states, "The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizen."[18] In this context, one is reminded of the objection of Warren & Brandeis to the yellow press of their day, "Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation, results in a lowering of social standards and of morality."[19]

Note too that Prosser in his article, *Privacy*, had originally proposed a tort standard of "offensiveness."[20] The Restatement process made the level for unreasonableness stricter by adding the word "highly" to the standard. Should tort law drop the concept of "highly offensive" and return to the original Prosser vision and prohibit publicity that is merely "offensive"?

---

[16] Restatement (Second) of Torts § 652D (1977) (comment h).
[17] On the question of legitimate public concern, Dean Robert Post views this concept as involving a search for matters of "public accountability." Robert Post, *The Social Foundations of Privacy*, 77 Cal. L. Rev. 958, 1008 (1989). In 1989, Post already pointed to a rise in the importance of "public accountability" against which privacy was fated to be of lesser weight. *Id*. at 1007.
[18] Restatement (Second) of Torts § 652D (1977) (comment c).
[19] Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890).
[20] William Prosser, *Privacy*, 48 Cal. L. Rev. 383, 396 (1960).

3. Intentional Infliction of Emotional Distress

One of Prosser's decisions for the privacy torts with lasting effects was to place the intentional infliction of emotional distress tort (IIED) into a separate section from privacy. That tort, as defined by the Restatement, provides: "One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm."[21]

While in a separate section, this tort bears many similarities to the privacy torts. As Neil Richards and Daniel Solove observe:

> The intentional infliction and privacy torts share many related features. Both are intentional torts, both provide a remedy for emotional injury, both rest on normative conceptions of unreasonable antisocial behavior, both are usually effected by words rather than actions, and both are products of tort law's expansion in the twentieth century to encompass psychological injuries rather than only physical injuries or injuries to property. Given these rather obvious similarities, one might think, therefore, that Prosser would have treated these related torts alike; indeed, many of the early tort cases are indistinguishable from intentional infliction claims.[22]

This list of similarities suggests that Prosser took a wrong turn by placing IIED in a separate part of the Restatement.

Would locating IIED into the same section as the privacy torts lead to a useful cross-fertilization in the case law regarding these torts? Does IEED belong in the same section as the privacy torts and made subject to an integrated analysis?

---

[21] *Id*. at § 46 (1977).
[22] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887 (2010).

4. Breach of Confidentiality

Another tort not included among the privacy torts was the breach of confidentiality tort (called "breach of confidence" in England). Breach of confidentiality was not included in Prosser's taxonomy of the privacy torts, and was not part of the privacy section of the Restatement (Second) of Torts. The breach of confidentiality tort provides a remedy whenever a person owes a duty of confidentiality and breaches the duty.

This tort was in existence prior to the Warren and Brandeis article. Indeed, Warren and Brandeis used a breach of confidence case from England – *Prince Albert v. Strange* – as the key precedent to support the right to privacy in the common law.[23] In England, *Prince Albert* spawned a robust jurisprudence, and one involving breach of confidence. At the same time, England has rejected the Warren and Brandeis privacy torts.[24] In America, in contrast, the breach of confidentiality tort remained stunted in its growth, and instead, a robust jurisprudence of privacy developed.[25] Yet, Warren and Brandeis never suggested supplanting the breach of confidentiality tort – they merely suggested augmenting it.

Despite the choice of Prosser and the Restatement, many states recognize the breach of confidentiality tort. One of its primary applications is in cases when healthcare providers breach confidentiality. It also applies to others who stand in fiduciary relationships, such as bankers and lawyers. While there is precedent in US law for a more robust breach of confidentiality tort, one should concede that the case law is relatively thin. In contrast, in England, the tort has widespread applicability; it applies to friends and family and others.

Should the breach of confidentiality tort be embraced more broadly and recognized in more situations in the US? Should it be part of the privacy section of the Restatement?

---

[23] Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193, 201-02, 204, 208 (1890).
[24] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality,* 96 Geo. L.J. 123, 145 (2007).
[25] Id. at 146-48.

The breach of confidentiality tort also has some important, positive differences from the privacy torts. One of the major limitations of the privacy torts has been that they often run afoul of the First Amendment.[26] Yet, the breach of confidentiality tort straddles the boundaries between contract and tort. As a result, it likely is free of the typical First Amendment limitations that regular torts have. Thus, recourse to this tort would provide privacy in situations where the privacy torts cannot due to constitutional concerns.

A further benefit of the breach of confidentiality tort is its absence of the "highly offensive" requirement found in many privacy torts. It lacks this test because it is focused not merely on the harms caused by the disclosure of secrets but on betrayal of a trusted relationship. As we have noted above, gossip blogs and other online fora may have reduced the ability of the judges applying the privacy tort to find certain publicity "highly offensive." As a result, the breach of confidentiality tort may be especially appealing in light of its absence of this requirement.

There is a final benefit of the tort of breach of confidentiality, which is its recognition of liability for the *inducer* of a breach of confidentiality. This result follows because this tort is derived from concepts of fiduciary duty. Indeed, both U.S. and English case law have assessed liability against such inducers of a breach. The tort can thus be quite potent, and it certainly has been in England where we see it operate in its full strength.

Should this tort now be included in the privacy section of the Restatement? If it were to take its place alongside the other privacy torts, courts might be inclined to recognize it more widely. While the tort seemingly would have been applicable in a number of privacy tort cases, neither litigants nor courts raised it in these actions. Many factors might have contributed to this phenomenon, but a simple explanation is that lawyers and judges are primarily familiar with the privacy torts through the Restatement and simply are unaware of the existence of the tort of

[26] For the private facts tort, for example, "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." See The Florida Star v. B.J.F., 491 U.S. 524 (1989). Also, for false light, actual malice is required. See Time, Inc. v. Hill, 385 U.S. 374 (1967).

breach of confidentiality. Few lawyers or judges specialize extensively in the privacy torts, so they are far less well known than many other garden-variety torts. Moreover, the spotlight on privacy remedies has been the privacy torts section of the Restatement. Including the breach of confidentiality tort would put it under this spotlight, where it might grow more robustly in the U.S. The inclusion of the breach of confidentiality tort among the privacy torts would go a long way to enhance the tort's recognition. Viewing this tort in connection with the other privacy torts would also shape its development as more lawyers considered this action in tandem with the other privacy torts. The result might be a view of interlocking and interrelated protections through the privacy torts and the breach of confidentiality tort.

5. Right of Publicity

There are other changes that are needed to the privacy torts. In our judgment, the privacy section of the Restatement should include the "right of publicity" tort, an offshoot of the appropriation tort.[27] The right of publicity is sometimes viewed as distinct from appropriation, and sometimes viewed as merely a dimension of the appropriation tort.

Neither Prosser nor the Restatement recognized a distinct tort of publicity.[28] We owe the right of publicity to Judge Jerome Frank's decision in 1953 in a case involving baseball cards. The doctrine originated in his opinion in *Haelan Laboratories v. Topps Chewing Gum, Inc.*, where the Second Circuit declared that "in addition to and independent of that right of privacy . . . a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture, and that such a grant may validly be made 'in gross,' i.e., without an accompanying transfer of a business or of anything else."[29] According to J. Thomas McCarthy, "while the appropriation branch of the right of privacy is invaded by an injury to the

[27] See generally J. Thomas McCarthy, The Rights of Publicity and Privacy (2000); Melville B. Nimmer, *The Right of Publicity*, 19 Law & Contemp. Probs. 203 (1954).
[28] See Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 220-23 (4th ed. 2011).
[29] 202 F.2d 866, 868 (2d Cir. 1953).

psyche, the right of publicity is infringed by an injury to the pocket book."[30] In other words, the appropriation tort is about privacy, and the right of publicity is about property.

The right of publicity is increasingly recognized by many jurisdictions. It is also best understood conceptually as a distinct tort. Such recognition would separate the privacy and property interests that are often confused in the application of the appropriation tort.

6. False Light

Another needed change concerns the formulation of the false light tort. The current formulation incorporates an actual malice standard – that "the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." This test is the First Amendment standard as articulated in a series of cases beginning with *New York Times v. Sullivan.*[31] Unlike the newsworthiness test of the public disclosure tort, this standard was not originally part of the tort itself. Rather, the Supreme Court grafted it onto the defamation torts. Indeed, there are also First Amendment standards and limitations on the other privacy torts, but these are not incorporated into the formulations of the tort. In contrast, with false light, the tort's formulation incorporates the U.S. Supreme Court's actual malice standard.

The problem with this standard is that the actual malice rule for false light has changed. The Restatement formulation was created after the Supreme Court decision in *Time, Inc. v. Hill* (1967), where the Court borrowed the actual malice standard from the defamation context and introduced it into the false light tort.[32] Subsequent to *Hill*, the Court decided *Gertz v. Robert Welch, Inc.* (1974).[33] In *Gertz,* the Court articulated a different standard from actual malice for private figures in defamation.

[30] J. Thomas McCarthy, The Rights of Publicity and Privacy § 5:61, at p. 5-110 (2000).
[31] 376 U.S. 254 (1964).
[32] 385 U.S. 374 (1967).
[33] 418 U.S. 323 (1974).

Although the Court never explicitly applied the *Gertz* rule to a false light case, courts are split in cases involving private figures as to whether *Gertz* applies to false light or whether all false light claims must satisfy the more stringent *New York Times* standard.[34] The better rule, in our opinion, is to apply *Gertz*, as the false light and defamation torts are quite similar, and there is no justification for false light exceptionalism.

The Restatement (Second) of Torts notes in a comment: "If *Time v. Hill* is modified along the lines of *Gertz v. Robert Welch*, then the reckless-disregard rule would apparently apply if the plaintiff is a public official or public figure and the negligence rule will apply to other plaintiffs.[35]

Because the fault standard for false light is contingent upon the public or private figure status of the plaintiff, the actual malice language should be removed from the tort's definition. It is not part of the definition, but it is part of the First Amendment.

7. Other Flaws of the Privacy Torts: Big Data, Data Security, Privacy Policies

A set of other shortcomings of the privacy torts should be mentioned. First, they have, by and large, failed to respond to the rise of "big data," having little applicability in this important context. Second, the privacy torts are not well designed to address data security breaches. Third, they are not applicable to violations of privacy policies.

Big data is a popular term that refers to companies designed around the information-rich environment in which we live. The McKinsey Global Institute defines "big data" as "datasets whose size is beyond the ability of typical database software tolls to capture, store, manage, and analyze."[36] As the Article 29 Working Group of the European Union has noted, "[W]e are witnessing a so-called 'data deluge' effect, where the amount of personal data that exists, is

[34] See, e.g., Braun v. Flynt, 726 F.2d 245 (5th Cir. 1984) (applying Gertz); Dietz v. Wometco West Michigan TV, 407 N.W.2d 649 (Mich. App. 1987) (applying Gertz); Dodrill v. Arkansas Democrat, 590 S.W.2d 840 (Ark. 1979) (applying New York Times); Schifano v. Greene County Greyhound Park, Inc., 624 So. 2d 178 (Ala. 1993) (applying New York Times).

[35] § 652E (comment d).

[36] McKinsey Global Institute, Big data: The next frontier for innovation, competition, and productivity 1 (May 2011).

processed and is further transferred continues to grow."[37] Big data companies include those involved in cloud computing and analytics. In cloud computing, as we have noted in our introduction, computing is delivered as a service. Analytics refers to the use of statistics, algorithms, and other tools of mathematics, which are then harnessed through information technology to use data to improve decision-making. In some instances, human decision-making may even be replaced by the use of analytics. As the McKinsey Global Institute states, "Decision making may never the same; some organizations are already making better decisions by analyzing entire datasets from customers, employees, or even sensors embedded in products."[38]

From all indications, the data deluge will not only continue, but increase, and the companies involved in collecting and analyzing big data will increase in importance.[39] These practices also create new kinds of threats to privacy and security. Yet, the privacy torts have little or nothing to say regarding these practices. For example, unauthorized access to data stored in the cloud is unlikely to give rise to a claim for intrusion upon seclusion. Once data are stored with a third party, an "intrusion" on them is unlikely to be considered as an invasion of "solitude or seclusion." The other privacy torts fit no better with concerns about big data and privacy. The use of analytics to make automated decisions is not likely to be found "highly offensive." Indeed, it is already an accepted business practice in many sectors.

---

[37] Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability 4 (July 13, 2010).

[38] McKinsey Global Institute, Big Data: The next frontier for innovation, competition, and productivity 5 (May 2011).

[39] In 2003, a study at the UC Berkeley School of Information found that the amount of new information being created every year and stored on media was 5 exabytes. Peter Lyman & Hal R. Varian, How Much Information? 2003 (University of California, Berkeley 2003), http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/. That amount is equal to the information stored in 37,000 libraries the size of the Library of Congress in the United States. By 2007, the amount of information stored each year had increased to 161 exabytes a year. Sharon Gaudin, The Digital Universe Created 161 Exabytes of Data Last Year, InformationWeek (Mar. 7, 2007), http://www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=197800. This development continues apace. In 2010, Google CEO Erich Schmidt noted that mankind now creates as much information every two days as it had from the dawn of civilization to 2003. MG Seigler, Eric Schimdt: Every 2 Days We Create as Much Information as We Did up to 2003, TechCrunch (Aug. 4, 2010), http://techcrunch.com/2010/08/04/schmidt-data/.

As for data security, there are now widespread concerns about leaks from the organizations with which we share our personal information. Due to numerous shortcomings, the privacy torts cannot be used as a tool in litigation to stop poor or insufficient data handling practices. Perhaps a new concept of privacy negligence is now needed, and we turn to this issue below.

8. Re-Igniting the Development of the Privacy Torts

Finally, the privacy torts have remained relatively unchanged following their codification in the Restatement of Torts (Second). Prior to that, the case law was developing in many different directions, but Prosser's codification of the privacy torts arguably has resulted in an ossifying effect. From this perspective, the Restatement ironically helped to promote the acceptance of the privacy torts in most jurisdictions, but also led to a cessation in their development.

Can the process of development be re-ignited? The torts are unable to address the privacy problems of today. If they are to remain more than a historical curiosity, they need to grow. Guidance and perhaps reformulation is thus needed.

Lior Strahilevitz has made an interesting proposal, which is to abandon the Prosser categories and replace them with a unitary tort for invasion of privacy. The key under the recast Strahilevitz privacy tort would simply be whether "the gravity of the harm to the plaintiff's privacy interest [is] outweighed by a privacy policy interest."[40] Would such an approach be workable?

[40] Lior Strahilevitz, *Reunifying Privacy Law*, 98 Cal. L. Rev. 2007 (2010).

B. Negligence, Strict Liability and Duties Owed Regarding Personal Data

The law of negligence has occasionally been invoked in the information privacy context, yet little work has been done to develop how negligence should work in this context. What duties, if any, should the entities that collect, use, and disclose personal data owe to the people to whom the data pertains?

Applicable case law shows different results when a negligent analysis is used in privacy cases. In *Huggins v. Citibank, N.A.,* the South Carolina Supreme Court held that a bank was not negligent for issuing a credit card in the plaintiff's name to a fraudster "without any investigation, verification, or corroboration" of the accuracy of the credit card application.[41] The South Carolina Supreme Court concluded that the defendant owed no duty to verify because "[t]he relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them."[42]

Other cases have reached different conclusions. In *Wolfe v. MBNA America Bank,* the plaintiff alleged that the defendant MBNA America Bank did not try to verify whether the information contained in a credit card application was authentic and accurate.[43] The plaintiff pointed to principles of negligence law. Specifically, the plaintiff argued that the defendant bank had a "duty to verify" the accuracy and authenticity of a credit card application sent in with plaintiff's name. The district court took issue with *Huggins:*

> Upon review, the Court finds the South Carolina Supreme Court's conclusion in *Huggins* to be flawed. In reaching its conclusion, the *Huggins* court relied heavily on the fact that there was no prior business relationship between the parties, that is, the plaintiff was not a customer of the defendant bank. The Court believes that the court's reliance on this fact is misplaced. While the existence of a prior business relationship might have some meaning in the context of a contractual dispute, a prior business relationship has little

[41] 585 S.E.2d 275 (S.C. 2003).
[42] *Id*. at 277.
[43] 485 F. Supp. 2d 874 (W.D. Tenn. 2007).

> meaning in the context of negligence law. Instead, to determine whether a duty exists between parties, the Court must examine all relevant circumstances, with emphasis on the foreseeability of the alleged harm.[44]

Thus, the *Wolfe* court set up a broad-based approach to assessing negligence.

The district court also noted that the limits of this duty to verify. The *Wolfe* court did not impose a strict liability duty on issuers of credit card to prevent all identity theft. Its negligence standard requires only reasonable steps to prevent identity theft. It stressed that its duty to verify required only "reasonable and cost-effective verification methods that can prevent criminals, in some instances, from obtaining a credit card with a stolen identity."[45] That issue was one for the trier of fact, whether judge or jury.

In another case, *Remsburg v. Docusearch, Inc*., the New Hampshire Supreme Court reached a rather bold and controversial conclusion regarding negligence.[46] In *Remsburg*, Defendant Docusearch, an information broker, provided personal information about a person to an individual who made an inquiry about her. That individual then used the data to locate the person and murder her. According to the *Remsburg* court, in certain limited circumstances, there is a duty to exercise reasonable care not to subject others to unreasonable harm. An "investigator," whether private investigator or information broker, has a duty of reasonable care when she discloses information to a client and thereby creates a foreseeable risk of criminal misconduct against the third person whose information is disclosed.

From the perspective of the Restatement on Torts, *Remsburg* opens a new and intriguing path for finding an affirmative duty when there is a "special relationship." The Restatement (Second) of Torts, § 315 states: "There is no duty so to control the conduct of a third person as to prevent him from causing physical harm to another." The exceptions are only when there is a "special relation," whether between the actor and the third person, that is the person causing the

[44] *Id*. at 881-82.
[45] *Id*. at 882.
[46] 816 A.2d 1001 (N.H. 2003).

harm, or between "the actor and the other which gives the other a right to protection." If a data broker's disclosure of data causes a person foreseeable harm, should this give rise to tort liability? How far should such a rule extend in the current information age?

Beyond negligence, some scholars have proposed strict liability for whenever personal data is used in ways that create harm to people. Danielle Citron argues that a strict liability regime is preferable to negligence tort liability:

> A negligence regime will fail to address the significant leaks that will occur despite database operators' exercise of due care over personal data. Security breaches are an inevitable byproduct of collecting sensitive personal information in computer databases. . . . .
>
> The high levels of residual risk suggest treating cyber-reservoirs as ultrahazardous activities — those with significant social utility and significant risk — that warrant strict liability. As Judge Richard Posner has explained, ultrahazardous activities often involve something "new" that society has "little experience" securing, where neither the injurer nor victim can prevent the accident by taking greater care. This characterized water reservoirs in nineteenth-century England. Strict liability creates an incentive for actors engaging in ultrahazardous activities to "cut back on the scale of the activity . . . to slow its spread while more is learned about conducting it safely."[47]

For Citron, "Just as no clear safety standard governing the building and maintenance of water reservoirs had emerged in the 1850s, a stable set of information-security practices has not yet materialized today."[48]

The Restatement (Second) of Torts proposes six factors for use in assessing the need for strict liability. These are: (1) the risk (probability) of harm was great; (2) the likelihood that the

[47] Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. Cal. L. Rev. 241 (2007).
[48] *Id*. at 266.

resulting harm if the risk materialized would be great; (3) such accidents could not be prevented by the use of due care; (4) the extent to which the activity was not a matter of common usage; (5) the activity was inappropriate to the place in which it occurred; and (6) the value to the community of the activity was outweighed by dangerous risks.[49] Despite the appeal of Citron's call for strict liability, it is unclear whether the Restatement test would find a need for strict liability for personal data processing. For one thing, the activity in question, namely the processing of personal data, is a matter of a matter of common usage. As another matter, the value to the community of the activity may be found greater than the danger.

How should the law of tort define the duties owed to people regarding the use and disclosure of their personal data? To what extent, if any, should strict liability be the standard for personal information processing and use?

[49] Restatement (Second) of Torts § 520 (1977).

C. Guiding Principles of Privacy Law

State legislatures are quite active in creating privacy law. This blizzard of legislative activity has led to an immense array of regulatory requirements for privacy and security. The state legislative activity has allowed for creative solutions and experimentation.

To draw on examples from a single state, we can point to a broad range of privacy and security laws from California. The following list, albeit extensive, is non-exhaustive:

- Cal. Fin. Code §§ 4050-4060, **Financial Information Privacy Act (SB1)**. Requires opt in for financial institutions sharing data with nonaffiliated companies. Permits financial institutions to offer incentives or discounts for people to opt in.
- Cal. Civil Code § 1747 et. seq, **Song-Beverly Act.** Prohibits retailers from collecting personally identifiable information from customers when completing credit card transactions. The California Supreme Court has found that this law extends to a request for a consumer's zip code at the time that a merchant completes a credit card transaction.[50]
- Cal. Civil Code §§ 1798.29, 1798.82, 1798.84, **Data Security Breach Notification.** Requires notification to individuals when a breach occurs involving their personal data. This California law, enacted in 2003, was the first such state law.
- Cal. Civil Code § 1798.81, **Data Disposal**. Requires a business to destroy personal information in a safe and effective fashion once it will no longer retain it.
- Cal. Civil Code § 1798.81.5, **Reasonable Security Practices.** Requires a business that owns or licenses personal information to implement and maintain reasonable security practices appropriate to the nature of the information to protect it from unauthorized access, destruction, use, modification, or disclosure.
- Cal. Business & Professions Code, 22948, **Anti-Phishing Law.** Prohibits using a Web page, email message, or any other means via the Internet to solicit, request, or take an

[50] Pineda v. Williams-Sonoma, 51 Cal. 4th 524 (2011).

action to induce an individual to provide identifying information by falsely representing herself as a legitimate business.

- Cal. Business & Professions Code, § 22575-22577, **Online Privacy Policy**. Requires commercial Website operators and online services that collect personally identifiable information about California residents to conspicuously post their privacy policy on their Website.
- Cal. Civil Code § 1798.83, the **"Shine the Light" Law**. Permits consumers to obtain from businesses information about the personal data that the businesses disclosed to third parties for direct marketing purposes.
- Cal. Insurance Code § 791 et sec. **Insurance Information and Privacy Protection Act**. Limits disclosure of personal information without the individual's written consent.
- Cal. Business & Professions Code D.8 §§ 22947 to 22947.6, **Anti-Spyware Statute**. Prohibits an unauthorized user from unwillfully loading spyware on the computer of a Californian and using this software to carry out a number of forbidden activities.
- Cal. Civil Code §§ 1749.64, **Supermarket Club Card Disclosure Act**. Prohibits club card issuers from selling or sharing a cardholder's name, address, telephone number, or other personal identification information unless certain conditions are met.
- Cal. Civil Code §§ 1798.79, Prohibits establishing a connection with a **Radio Frequency Identification Tag** without explicit consent from the tag's owner.
- Cal. Civil Code §§ 1936(o)-(p), **Electronic Surveillance Technology: Rental Cars**. Prohibits a rental car company from using, accessing, or obtaining any information relating to a renter's use of the vehicle obtaining using electronic surveillance technology, such as a Global Positioning System (GPS), wireless technology, or a location-based technology. Certain exceptions are provided for in the statute.

California also has its own institutional structure for privacy. In June 2012, California Attorney Kamala D. Harris established a Privacy Enforcement Unit in the state's Department of Justice. There is also a Director of Privacy Education and Policy in the new Privacy Enforcement Unit; the Director will oversee consumer education and outreach to industry.

California also has a longstanding Office of Privacy Protection, which promotes the privacy of consumers.[51]

Different states have different packages of privacy laws. The result of these state privacy laws is a complicated and confusing landscape for companies engaged in business throughout the US. Yet, state privacy law has never been of greater importance because of gridlock in Congress and the lack of any recent Federal privacy legislation. It is likely that there will continue to be an absence of needed federal action in important areas, such as data breach notification legislation.

Thus, with this lack of leadership from Congress, and little expected from it in the near future, the states have risen to a new level of power and influence when it comes to regulating privacy. Is there a way for improved state coordination and consistency in regulating privacy? The Restatement (Second) of Torts created substantial uniformity in the way states defined the privacy torts. Currently, there are no benchmarks for states that indicate the types of laws that are needed to protect information privacy. In the absence of guidance, we see various state laws enacted with very different levels of protection.

A new set of guidelines might help serve as a blueprint for states to adopt more consistent privacy legislation. Such guidelines would define the basic areas for coverage – the particular issues that require a privacy law – as well as the basic parameters for how, substantively, these issues should be addressed. We propose developing a blueprint for state privacy legislation, a set of guidelines that set forth the areas that ought to be covered and the basic substantive provisions that ought to be included. What is the ideal package of state privacy laws?

[51] California Office of Privacy Protection, About the Office of Privacy Protection, at http://www.privacy.ca.gov/about_us/index.shtml. As the Office of Privacy Protection explains its non-enforcement role, "Our mission is to identify consumer problems in the privacy area and encourage organizations from businesses to governments to develop fair information practices."

D. Data Security Breach Notification

The vast majority of states have data security breach notification laws. The current tally is that forty-six states have such statutes. Each law, however, is different, making compliance quite complicated for companies doing business across the United States. For example, the definition of personal information in different statutes can vary. As one treatise on privacy law states, "Many states have varied the definition of personal information to include … any number of … potentially identifiable data elements."[52] This treatise also notes "important variations among the states as to what triggers a requirement to notify affected individuals."[53] State laws also vary as to who must be notified in the event of a breach, and the kinds of information that are to be given to these parties.

Despite discussion of the issue, Congress has yet to enact a broad-based federal data security breach notification statute. There is a limited federal notification requirement found in the Health Information Technology for Economic and Cultural Health (HITECH) Act of 2009. Under the HITECH Act, an entity that is covered by HIPAA, the Health Insurance Portability and Accountability Act, must notify affected individuals if it experiences an information security breach involving "unsecured protected health information."[54] HITECH contains a broad definition of "breach," which it defines as "unauthorized acquisition, access, use or disclosure of protected health information."[55]

There are also important differences among the various data breach notification laws regarding the extent of any obligation to share information with a central authority. Some state data breach notification statutes "require that the organization notify the state attorney general or

[52] Lisa J. Sotto, Privacy and Data Security Law Deskbook 15-4 (2011).
[53] Id. at 15-5.
[54] HITECH Act, §13402(a). The term "protected health information" includes all "individual identifiable health information" transmitted by or maintained in electronic media or any other form or medium. HITECH Act, §13400(12); 45 C.F.R. § 160.103.
[55] HITECH Act, § 13400(1).

another state agency (in addition to the affected individuals and consumer reporting agencies)."[56] The HITECH Act requires that if the breach affects 500 or more individuals, the HIPAA covered entity is required to provide notice to the Department of Health and Human Services.[57]

Many questions are open about breach notification statutes. Notification is quite costly. In an incident involving a medical records company, required data breach notification was so costly that the organization was forced into bankruptcy.[58] At the same time, it is not clear whether notification is an effective means to protect consumers. Fred Cate is one of the leading critics of breach notification laws as they are currently structured. In his view, the flood of notifications to consumers has taught consumers to ignore these messages.[59]

It is also an open question whether there is adequate oversight of how the breach notification process works. In 2007, Paul Schwartz and Edward Janger called for the development of a "coordinated response agent" that, among its other tasks, would share information about data security breaches, oversee the response of private sector entities, and supervise the decision of breached entities whether or not to disclose to consumers."[60] While some state laws have taken steps in this direction, much more could be done to improve the coordination of breach notification.

What should the rules be for notification? Is there a preferable standard? Since Congress appears unlikely to enact federal data security breach notification legislation, what can state legislatures do to provide for greater consistency? An ALI set of standards would be a means to establish reasonable and effective standards for breach notification.

---

[56] Lisa J. Sotto, Privacy and Data Security Law Deskbook 15-7 (2011).
[57] HITECH Act, § 13402(e)(2).
[58] Burglary Triggers Medical Records Firm's Collapse, Wall St. J. (March 12, 2012), at http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm%E2%80%99s-collapse/tab/print/
[59] Fred Cate, Another notice isn't answer, USA Today, Feb. 27, 2005, at 14A.
[60] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 Mich. L. Rev. 913, 955 (2007).

E. Beyond Notice and Choice

An approach known as "notice and choice" is the predominant way that the law protects the privacy of consumer information in business records. The idea behind notice and choice can be summarized in this fashion: As long as a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected. This choice is not a robust right, but instead often merely provides the ability to opt out of some information uses.

When Internet e-commerce took off in the mid-1990s, many companies created privacy policies that stated their practices with regard to the collection, use, and dissemination of personal data. These companies also offered people the ability to opt out of certain uses or disclosures of their information. This approach helped industry ward off federal and state legislation. Congress passed a few targeted laws to protect privacy in certain sectors, such as the Video Privacy Protection Act,[61] which addresses the privacy of people's video entertainment choices, and the Cable Communications Policy Act,[62] which safeguards the privacy of cable records. But for most consumer information, such as data collected by merchants, supermarkets, bookstores, and restaurants, Congress has yet to enact any sectoral laws.

Even existing laws that regulate privacy rely heavily on notice and choice. For example, the Children's Online Privacy Protection Act works primarily by requiring companies to have privacy policies to put parents on notice of how their children's data will be used and to give them the choice to opt out, or indicate their refusal to "permit the operator's future use or maintenance in retrievable form, or future online collection, of personal information from that child."[63]

Instead of enactment of a full range of "fair information practices" in a broad-based bill that covers the use and processing of personal data, regulators in the U.S. have predominately

[61] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.
[62] Cable Communications Privacy Act of 1984, 47 U.S.C. § 551.
[63] Children's Online Privacy Protection Act, 15 U.S.C. § 6502(b)(1)(B).

relied on the notice and choice approach. Fair information practices are a number of basic information privacy principles that allocate rights and responsibilities in the collection and use of personal information.[64] This path continued to be followed even after the EU Data Protection Directive raised vexing issues for the transfer of data between the United States and the European Union. The EU requires that countries to whom data is transferred provide an "adequate level" of privacy protection. A Safe Harbor Agreement was established to enable data transfers between EU countries and the United States.[65] The Safe Harbor Agreement endorsed the notice and choice approach, a decision that received significant criticism in both the EU and United States.

Notice and choice is by and large a self-regulatory approach. Companies are free to make whatever substantive promises they desire. Businesses can offer the consumer no privacy, bad levels of privacy, or strong privacy. The only consequences that companies face will occur should they violate the promises made in their privacy policies. Even some broken promises, however, go without penalty. The notice and choice approach is simply too voluntary for industry, and depends upon companies restricting their own behavior. The problem is that the good apples will do so, but the bad apples will not.

Thus, a major problem with notice and choice is that it lacks any substantive restriction on what companies may do with personal information. All it requires is that companies follow their promises. But companies need not promise anything of note. This problem is becoming especially acute for "apps" – applications used by smart phones and websites. App developers are often small start-ups in a basement or a garage that know nothing about privacy law or best privacy and security practices. Many apps gather extensive personal data. Yet they exist without any privacy policy.

An additional major problem with notice and choice is that notice is illusory in practice. Privacy policies are long, cumbersome, and hard to read. Indeed, most people do not read privacy policies.

[64] Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 37 (4th ed. 2011).
[65] Export.gov, http://export.gov/safeharbor/.

Moreover, privacy policies are often vague and unclear because they are drafted with the companies' self-interest in mind. There is little incentive for a company to provide specific notice as it will narrow that company's future potential use of information. Put differently, it is in the self-interest of companies to keep open their options, present and future, regarding use of personal information.

On the choice side of notice and choice, some companies view choice as resting on allowing its customers the ability to opt out of certain data sharing and uses. Opt out sets the default as the company's right to use data however it desires unless a consumer indicates she does not want her data used or disclosed. Consumers can opt out by checking a box or taking other actions to indicate their "choice."

As for opt out, the problems with it are legion. Companies have no incentive to make opting out easy, and every incentive to make it difficult. As a result, opt out is often cumbersome. Some companies will refresh people's preferences periodically, requiring them to opt out again and again if they want to remain opted out. Studies show that most people do not opt out – indeed, hardly anybody opts out – which is why companies prefer opt out so much.[66] It allows companies to shift burden and blame to consumers.

Should notice and choice be replaced with a different regulatory regime?

[66] Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 Vand. L. Rev. 1583 (1998) (observing that most people accept default terms).

F. Harmonization with International Law

The current law of privacy is fragmented in several ways. Internationally, the United States's approach to privacy diverges from those of Europe and many other countries. In the US, privacy law is sectoral. Different laws with different standards apply to different industries.

People often think that certain types of data are protected or unprotected by privacy law, but thinking in terms of types of data is not consistent with how US privacy regulation works. Rather, US privacy law frequently regulates personal information by types of data holder. As an example, medical information as a category does not receive a uniform level of protection. If it is held by a "covered entity" under HIPAA, it is protected by one set of rules. If it is held by a school regulated by FERPA, it is subject to a different set of rules. And if it is held by neither, it might not be protected at all. As a final example, the Fair Credit Reporting Act (FCRA) provides privacy protections for consumer information held by credit bureaus. Among its protections, FCRA requires that credit bureaus permit a consumer access to her credit report. There is no such legal right, however, to see the financial or credit-related information that a database marketing company maintains about a person.[67]

The EU, in contrast, has an omnibus approach that protects data no matter who holds it, though there are some variances in the law. Another important aspect of EU data protection law concerns the need for an adequate legal basis before personal information can be processed. For example, German law expresses this concept as a "*Verbot mit Erlaubnisvorbehalt*," or a "prohibition with conditional permission."[68] EU law starts by forbidding the collection, processing, or use of personal data. This prohibition is lifted, however, once a legal authority authorizes the data collection, processing, or use in question.

[67] Natasha Singer, Consumer Data, But Not for Consumers, N.Y. Times, Sunday Business 3 (July 22, 2012).
[68] See the German Federal Data Protection Law [Bundesdatenschutzgesetz] [BDSG] of Jan. 14, 2003 (BGBl. I [Federal Reporter I] at 66).

This starting point presents a notable contrast with the approach in the United States. The United States generally permits the use of personal information unless a law prohibits it. This orientation is due, in part, to the strong First Amendment protections for freedom of expression.

In addition, in the US, much privacy regulation is based in part on a self-regulatory approach, where companies provide privacy notices that make certain promises about privacy. If these promises are violated, the FTC might penalize the company. But the FTC's power generally extends only to the promises made, so a company can determine how stringently it wants to protect privacy by modulating the promises it makes. In many instances, people are given only a right to opt out of certain uses of their data, and often have no right at all to limit the collection of data about themselves. In the EU, moreover, the rules regarding individual consent for data collection, use, and disclosures are much stricter.

As a further limitation in the US, privacy legislation exists for certain industries but each industry's legislation is different, and many repositories of data are not regulated. Thus, and as noted above, US law regulates credit bureaus, but does not regulate data brokers. In the EU, in contrast, there is extensive regulation on all data processors: in the terminology of information privacy, Europe relies on omnibus law rather than sectoral ones. As Joel Reidenberg notes, "the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector. Legal rules have developed on an ad hoc, targeted basis, while industry has elaborated voluntary norms and practices for particular problems."[69]

With the new EU proposed legislation, the Draft Data Protection Regulation (2012), the clash between the US and EU approaches to privacy has never been more tense.[70] The Draft Regulation appears to double down on the earlier approach of the 1995 EU Directive on Data

[69] Joel R. Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, 80 Iowa Law Review 497, 500 (1995).
[70] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Jan. 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

Protection. It proposes a right to be forgotten, more explicit consent requirements for data processing, and stronger enforcement powers for EU regulators.

At the same time, the Obama Administration is seeking to close the gap between the US and EU. In February 2012, it issued a Privacy Blueprint, which, among its other goals, sought greater "interoperability" between international privacy regimes.[71] Its central focus was on how U.S. companies engaged in international business could continue to have access to "the free flow of information" across borders.[72] Towards this goal, the White House sought "increased interoperability between the U.S. data privacy framework and those of our trading partners." The Obama Administration built its vision around "mutual recognition of privacy frameworks," an "international role for codes of conduct," and "enforcement cooperation."[73]

The White House's chosen concept of interoperability has a subtle implication: if the rest of the world and the American privacy systems interconnect, an international exchange of personal information could occur without difficulties. Yet, both sides of the Atlantic have great skepticism about the other side. Many in the US view the EU approach as unreasonable and stifling useful information flow. Many in the EU view the US approach as unprincipled, inimical to individual dignity, and essentially the equivalent of hardly any regulation at all.

Can there be a reconciliation between these two approaches? How can we reconcile the approaches? Can we come up with a core of shared privacy principles that the world can acce

[71] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[72] Id. at 33.
[73] Id. at 31.

III. PUBLIC LAW PROJECTS

A. Privacy and Free Speech

The recent case of *Sorrell v. IMS Health* involved a Vermont privacy statute struck down for violating the First Amendment.[74] The statute restricted the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual physicians. The Supreme Court declared, "[s]peech in the aid of pharmaceutical marketing . . . is a form of expression protected by the Free Speech Clause of the First Amendment."[75] It subjected the law to heightened judicial scrutiny and found that it could not meet this standard. For the *Sorrell* Court, "the creation and dissemination of information are speech within the meaning of the First Amendment."[76] Vermont's content- and speaker-based restrictions on the use of prescriber-identifying information were found to be unconstitutional.

After *Sorrell*, there is new uncertainty about the relationship between the First Amendment and information privacy law. The conflict between the First Amendment and privacy has occurred in other settings as well. For example, in *Trans Union v. FTC*, a company sued to enjoin FTC regulations promulgated pursuant to the Gramm-Leach-Bliley Act.[77] The conflict concerned restrictions on the ability of Trans Union to sell credit headers, which consist of a consumer's name, address, Social Security Number, and phone number. For Trans Union, the sale of credit headers was "commercial speech." For the D.C. Circuit, however, the government had a substantial interest in protecting the privacy of consumer credit information and it upheld the FTC's action.[78]

In the academic literature, there is no consensus about the permissible kinds of speech-related protection that the collection, use, and/or transfer of personal information should receive. For example, Eugene Volokh considers such data processing as constituting speech, which deserves strong First Amendment protection. He contends, "The owners and managers of a

[74] 131 S. Ct. 2653 (2011).
[75] Id. at 2659.
[76] Id. at 2667.
[77] 295 F.3d 42 (D.C. Cir. 2002).
[78] In reaching this decision, the D.C. Circuit relied on its earlier decision, Trans Union Corp. v. Federal Trade Commission, 245 F.3d 809 (D.C. Cir. 2001).

credit bureau are communicating information to decisionmakers, such as loan officers, at the recipient business."[79] Volokh views many information privacy laws as unconstitutional. In contrast, Daniel Solove argues, "There are no easy analytic distinctions as to what is or is not 'speech.' . . . . It is the *use* of the information that determines what information is, not anything inherent in the information itself."[80] For Paul Schwartz, it is important to remember that free discourse is promoted by the protection of privacy.[81] In other words, privacy can further the goals of the First Amendment. He also argues that many aspects of information privacy legislation do not silence or restrict speech.

Due to the unsettled state of this area of constitutional law, Congress and state legislatures face uncertainty when enacting privacy laws. A valuable ALI project would develop principles for use in drafting privacy legislation without violating the First Amendment.

[79] Eugene Volokh, *Freedom of Speech and Information Privacy*, 52 Stanford L. Rev. 1049, 1093-1094 (2000).
[80] Daniel J. Solove, *The Virtues of Knowing Less*, 53 Duke L.J. 967, 979 (2003).
[81] Paul M. Schwartz, *Free Speech vs. Information Privacy*, 52 Stanford L. Rev. 1559 (2000).

B. Intellectual Privacy and Anonymity

Professor Neil Richards, a law professor at Washington University School of Law, has coined the term "intellectual privacy" to describe the special subgroup of sensitive personal data relating to our consumption of ideas, our speech, and our reading habits.[82] Other scholars, such as Julie Cohen and Paul Schwartz, have traced the ways that privacy can promote social discourse.[83]

As an example of intellectual privacy in action, the law of most states has special protections for library records. The Internet is a library of sorts, where people can search for an astounding array of information, including books. Should the law be tethered to the libraries of old?

What should the boundaries of intellectual privacy be in the 21st Century? Should the law protect intellectual privacy differently than other kinds of privacy?

In a fashion related to intellectual privacy, anonymous speech can promote communication. At the same time, however, an issue that comes up frequently involves the anonymity of speakers that engage in potential defamation, cyberbullying, harassment, privacy invasions, and other activities that harm others. Such speakers often communicate under the veil of anonymity. When should such speakers be unmasked?

Courts have applied at least four different types of standards to protect the free speech rights of anonymous speakers:

[82] Neil Richards, *Intellectual Privacy*, 87 Tex. L. Rev. 387 (2008).
[83] Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 Stanford L. Rev. 1373 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vanderbilt Law Review 1609 (1999).

1. *Summary Judgment Standard.* Under this standard, a plaintiff must establish that the case would survive a summary judgment motion.[84]

2. *Motion to Dismiss Standard.* Under this standard, a plaintiff must establish that the case would survive a motion to dismiss.[85]

3. *The Prima Facie Case Standard*. According to this standard, the plaintiff must produce evidence showing a prima facie case on all elements and must demonstrate that revealing the identity of the anonymous speaker will not severely harm the speaker's free speech or privacy rights and will be "necessary to enable plaintiff to protect against or remedy serious wrongs."[86]

4. *The Variable Standard*. This standard varies depending upon the nature of the speech, with commercial speech being protected by a much lower standard than non-commercial speech.[87]

These standards vary considerably in their strength and balance the interests of free speech and plaintiffs' rights quite differently. Greater uniformity is needed.

Speakers on the Internet will not know the level of anonymity protection that the law provides, as it will depend upon the jurisdiction in which a plaintiff may decide to litigate.

[84] Doe v. Cahill, 884 A.2d 451 (Del. 2005).
[85] Columbia Insurance Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).
[86] Highfields Capital Mgmt., LP v. Doe, 385 F. Supp. 2d 969 (N.D. Cal. 2005); Dendrite Int'l v. Doe No. 3, 775 A.2d 756 (N.J. Super. App. Div. 2001).
[87] In re Anonymous Online Speakers, 611 F.3d 653 (9th Cir. 2010) (known as the "Quixtar" case).

IV. MIXED PRIVATE LAW/PUBLIC LAW PROJECTS

A. Defining PII

Personally Identifiable Information (PII) is a central concept in privacy regulation. It defines the scope and boundaries of a large range of privacy statutes and regulations. Numerous federal statutes turn on this distinction.[88] Similarly, many state statutes also rely on PII as a jurisdictional trigger.[89] These laws all share the same basic assumption—that in the absence of PII, there is no privacy harm. Thus, privacy regulation focuses on the collection, use, and disclosure of PII, and leaves non-PII unregulated.

Given PII's importance, it is surprising that information privacy law in the U.S. lacks a uniform definition of the term. In addition, computer science has shown that the concept of PII is far from straightforward. Increasingly, technologists can take information that appears on its face to be non-identifiable and turn it into identifiable data.

Given the ubiquity of the concept of PII in privacy law and the important role it plays, the definition of PII is crucial. But instead of defining PII in a coherent and consistent manner, privacy law offers multiple competing definitions, each with significant problems and limitations. There are three predominant approaches to defining PII in various laws and regulations. These approaches are (1) the "tautological" approach, (2) the "non-public" approach, and (3) the "specific-types" approach.

The tautological approach is an example of a standard, and it defines PII as any information that identifies a person. The Video Privacy Protection Act (VPPA) neatly demonstrates this model.[90] The VPPA, which safeguards the privacy of video sales and rentals, simply defines "personally identifiable information" as "information which identifies a

[88] Examples include the Children's Online Privacy Protection Act, the Gramm-Leach Bliley Act, the HITECH Act, and the Video Privacy Protection Act.
[89] Examples include California's Song-Beverly Credit Card Act and the numerous state breach notification laws.
[90] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

person."[91] For purposes of the statute, information that identifies a person is PII and falls under the statute's jurisdiction once linked to the purchase, request, or obtaining of video material.

The problem with the tautological approach is that it fails to define PII or explain how it is to be singled out. At its core, this approach simply states that PII is PII. As a result, this definition is unhelpful in distinguishing PII from non-PII.

A second approach to defining PII is to focus on non-public information. The non-public approach seeks to define PII by focusing on what it is *not* rather than on what it is. Instead of saying that PII is simply that which identifies a person, the non-public approach draws on concepts regarding information that is publicly accessible and information that is purely statistical. This model would exclude information that falls in these categories from PII, but the relevant legislation does not explore or develop the logic behind this approach. The Gramm-Leach-Bliley Act epitomizes one aspect of this approach by defining "personally identifiable financial information" as "nonpublic personal information."[92] The statute fails to define "nonpublic," but presumably this term means information not found within the public domain.

The problem with the non-public approach is that it does not map onto whether the information is in fact identifiable. The public or private status of data often does not match up to whether it can identify a person or not. For example, a person's name and address, which clearly identify an individual, nevertheless might be considered public information, as such information is typically listed in telephone directories. In many cases, however, individuals have non-public data that they do not want matched to this allegedly public information. Yet, an approach that only protects non-public information as PII might not preclude such combinations.

The third approach is to list specific types of data that constitute PII. In the context of the specific-types approach, if information falls into an enumerated category, it becomes "per se" PII

[91] Id. § 2710(a)(3). The VPPA prohibits "videotape service providers" from knowingly disclosing personal information, such as the titles of items rented or purchased, without the individual's written consent. It defines "videotape service providers" in a technological neutral fashion to permit the law to be extended to DVDs. Id. § 2710(a)(4).
[92] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2006).

by operation of the statute. As an example, we can consider the Children's Online Privacy Protection Act (COPPA), which regulates the collection and use of children's information by Internet websites or online services.[93] COPPA states that personal information is "individually identifiable information about an individual collected online," including first and last name, physical address, social security number, telephone number, and e-mail address.[94]

The specific-types approach can be quite restrictive in how it defines PII. It can also assume that the types of data that are identifiable to a person are static, and there is no need to cover information that could potentially become personally identifiable.

PII remains a central concept in privacy regulation. It strikes many as common sense that a person's privacy can be harmed only when PII is collected, used, or disclosed. Nonetheless, PII, as currently defined, is a troubled concept for framing privacy regulation. In particular, the current distinction between PII and non-PII proves difficult to maintain. Indeed, whether information is identifiable to a person will depend upon context and cannot be determined *a priori*.

Thus, the law needs a reconceptualized notion of PII. But how is PII 2.0 to be defined? In its long awaited 2012 report, *Protecting Privacy in an Era of Rapid Change*, the FTC stated that its proposed framework applies to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."[95] It held that "the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine that data's privacy implications."[96]

In a related but distinct approach, we have argued that identifiability should be defined as continuum of risk rather than as a simple dichotomy. [97] Our model of PII 2.0 is also more

[93] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006).
[94] *Id*. § 6501(8)(A)–(E).
[95] FTC, Protecting Consumer Privacy in an Era of Rapid Change 18 (March 2012).
[96] *Id*. at 19.
[97] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.REV. 1814 (2011), available at http://ssrn.com/abstract=1909366.

detailed than the FTC's. The key to our model is to build two categories of PII, "identified" and "identifiable" data, and to treat them differently. Furthermore, PII 2.0 introduces a scaled protection dependent on the sensitivity of the data. This approach permits tailored legal protections built around different levels of risk to individuals.

How are categories of identified and identifiable information to be maintained? What is the best approach for the law in defining PII?

B. Systematic Data Access

There has been a shift in the fashion in which the government gains access to private sector information. Much of this access now occurs not through a warrant or other formal demand for information about a specific individual. Rather, there is more information that is being collected and shared on a regular, that is, systematic basis. As one analysis of the issue stated, "The ways in which systematic government access may operate are rarely transparent, often presenting themselves only when a controversy surfaces in the press, as in the case of the Terrorist Surveillance Program (an NSA program where, without any court order, the NSA, assisted by major telecommunications companies, intercepted communications when at least one party was located in the United States)."[98]

Beyond the NSA's controversial Terrorist Surveillance Program, "fusion centers" offer another example of systematic data access. As Danielle Citron and Frank Pasquale have explained:

> Federal agencies, including the DHS, gather information in conjunction with state and local law enforcement officials in what Congress has deemed the "information sharing environment" ("ISE"). The ISE is essentially a network, with hubs known as "fusion centers" whose federal and state analysts gather and share data and intelligence on a wide range of threats.[99]

There are now seventy-two such centers. Private entities help run fusion centers and are co-located within these entities. As Citron and Pasquale note, private firms now increasingly send their employees to work at fusion centers.[100] What should the rules be to create accountability for government systematic access to personal data?

---

[98] Stephanie Pell, *Systematic Government Access to Private-Sector Data in the United States*, forthcoming 3 International Data Protection Law – (2013).
[99] Danielle Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 Hastings L.J. 1441, 1443 (2011).
[100] Id. at 1449.

C. Drones

There will be increased use of drones, also known as unmanned aerial vehicles, in the US in years to come. The Federal Aviation Administration Modernization and Reform Act of 2012 requires the Federal Aviation Administration to develop a plan "to accelerate the safe integration of unmanned aircraft systems (UAS) into the national airspace system" by September 30, 2015.[101] Already some law enforcement agencies and private organizations are using drones.

At present, there is scant legal regulation, or useful legal doctrine that restricts use of this technology. Moreover, the drone industry's sole attempt at self-regulation is a broadly written code of conduct without any real restrictions on drone use.[102] Ryan Calo warns, **"**That drones will see widespread domestic use seems inevitable. They represent an efficient and cost-effective alternative to helicopters and airplanes."[103] Calo also comments, "Imagine what drones would do for the lucrative paparazzi industry, especially coupled with commercially available facial recognition technology."[104] Jonathan Zittrain thinks that drones are a "game changing" technology.[105] He writes, "People can become recognizable by their unique gaits; anyone walking could be located at a particular place and time. Car license plates can be read, as perhaps could (cracked) toll booth fast pass IDs."[106]

How should drones be regulated for law enforcement use? Should there be a warrant regulation for their use? How should drones be regulated for the private sector? Are anti-stalking laws and anti-paparazzi laws useful models for this context?

---

[101] H.R. CONF. REP. No. 112-381 196-97 (2012).
[102] Association for Unmanned Vehicle Systems International, Unmanned Aircraft System Operation, Industry Code of Conduct (2012). For criticism of the Code of Conduct, see Jaikumar Vijayan, Drone industry's Code of Conduct disappoints, Computerworld Blogs (July 12, 2012), at http://blogs.computerworld.com/privacy/20685/drone-industrys-code-conduct-disappoints.
[103] M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 Stanford L. Rev. Online 29 (2011), at http://www.stanfordlawreview.org/online/drone-privacy-catalyst.
[104] Id.
[105] Jonathan Zittrain, These Aren't Just Toy Planes, N.Y. Times (Feb. 20, 2012), at http://www.nytimes.com/roomfordebate/2012/02/20/civilian-drones-in-the-united-states/civilian-drones-arent-just-toy-planes.
[106] Id.

D. Defining Privacy Harms

Courts have struggled with the proper definition of a privacy harm. For example, in the recent case *FAA v. Cooper*, the U.S. Supreme Court held that the Privacy Act did not recognize psychological harms as solely sufficient to create an actual injury.[107] The *Cooper* Court's reluctance to find actionable harms from privacy invasions is representative beyond its particular statutory context. For example, courts are often skeptical of privacy tort actions that point only to emotional or mental harms. In 2003, Joel Reidenberg concluded an analysis of privacy enforcement actions by observing, "privacy remedies for personal wrongs are not easily accommodated within the existing set of legal rights."[108] A similar judgment can be reached in 2012.

At the birth of privacy law in the US, marked by the Warren and Brandeis article of 1890, such a restrictive view of privacy harms was not present. Warren and Brandeis wrote that privacy harms involved an "injury to the feelings."[109] Privacy harms, they noted, can subject people to "mental pain and distress far greater than could be inflicted by mere bodily injury."[110]

Despite the growth of the intentional infliction of emotional distress tort and the privacy torts, courts in privacy cases still struggle to recognize that only emotional or psychological harm can form a basis for a lawsuit. As an example of such difficulty, most cases involving data security breaches have concluded that there is no harm from leaked data unless it causes identity theft. There are at least three general bases upon which plaintiffs argue they are injured by a data security breach:

---

[107] FAA v. Cooper, 132 S. Ct. 1441, 1453 (2012) ("[T]he term 'actual damages' can include nonpecuniary loss. But this generic meaning does not establish with the requisite clarity that the Privacy Act, with its distinctive features, authorizes damages for mental and emotional distress.").
[108] Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877, 892 (2003).
[109] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 197 (1890).
[110] Id. at 196.

1. The exposure of their data has caused them emotional distress.[111]

2. The exposure of their data has subjected them to an increased risk of harm from identity theft, fraud, or other injury.[112]

3. The exposure of their data has resulted in their having to expend time and money to prevent future fraud, such as signing up for credit monitoring, contacting credit reporting agencies and placing fraud alerts on their accounts, and so on.[113]

Courts have rejected all three of these arguments. Yet, in these data security breach cases, courts do *not* dismiss claims because companies practiced reasonable security and were not negligent. Indeed, the companies may have been grossly negligent, or even reckless, without being found to be liable.

As a final example of the troublesome current doctrinal state of privacy harms, an FTC Staff Report wondered in 2010 whether the agency's "harm-based approach" was too limited.[114] Beyond the narrow set of harms that the FTC had already identified in its privacy enforcement actions, the Staff Report observed that "the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'"[115] The Staff Report's call to move beyond the FTC's "harm-based approach" has not garnered much support. Indeed, it provoked an immediate and negative reaction from one Commissioner in a separate statement added to the 2010 Report.[116]

[111] See, e.g., Doe v. Chao, 540 U.S. 614 (2004).
[112] See, e.g., Ruiz v. Gap, Inc., 622 F. Supp.2d 908, 913 (N.D. Cal. 2009) ("While [the plaintiff] has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law.").
[113] See, e.g., Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006).
[114] FTC, Protecting Consumer Privacy in an Era of Rapid Change, Preliminary FTC Staff Report, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[115] Id. at 20.
[116] Id. at Appendix E.

What is the harm created by a privacy violation? Is it a leak of personal data? How should such harms be measured and defined? In *Understanding Privacy* (2008), Daniel Solove identified several types of potential privacy harms. These are physical injuries; financial losses and property harms; reputational harms; emotional and psychological harms; relationship harms; vulnerability harms; chilling effects; and power imbalances. Should the law protect against injuries to all these interests?

E. Education Privacy

Education privacy is in disarray. In contrast to schools, companies in many industries have chief privacy officers and a privacy program. These programs involve assessments of privacy risks, training, updating policies, and a point person tasked with handling questions and problems regarding privacy.[117] Only a handful of institutions of higher education have privacy officers, and hardly any K-12 school has a privacy officer.

The law of education privacy has been dominated by the federal Family Educational Rights and Privacy Act (FERPA), a law passed in 1974.[118] It is now woefully outdated. As an example, the statute's central concept is "education records" rather than PII.[119] FERPA defines education records as "information directly related to a student" that an educational institution itself "maintain[s]" in a file or other record.[120] Thus, the statute's coverage depends on whether or not a school has first organized and then stored data in "education records."[121]

Due to FERPA's limitations, schools long profited by distributing "surveys" on behalf of marketers. Since the collected information went from parents and children to marketers without being "maintain[ed]" in "educational records" by schools, this practice fell outside of FERPA's coverage. Congress finally responded to this practice in a modest fashion in 2005. It left FERPA unaltered, but created a limited separate statutory interest that permits parents of elementary and secondary school students to opt out of the collection of student information for commercial purposes. Congress neither revisited FERPA's reliance on the concept of "educational records," nor created a more basic right to block the release of student records for

[117] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011).
[118] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.
[119] 20 U.S.C. § 1232g(b)(2).
[120] *Id.*
[121] In 2002, in Owasso Independent School District v. Falvo, 534 U.S. 426 (2002), the Supreme Court went further than even FERPA's statutory language and strongly suggested in dicta that FERPA records are only those kept in a permanent file and by a "central custodian" at the school. Id. at 434–35.

commercial purposes.[122] As for universities, they remain able to sell essential student contact information to credit card companies. Such data is considered "directory information," and hence not an "education[al] record."[123]

A further flaw in FERPA is that it contains only one, extreme sanction, which is withdrawal of all federal funding for the educational institution.[124] This penalty is impractical due to its draconian nature. In fact, such a penalty has never been assessed in the history of the law.

Education is an area with poor and incomplete privacy regulation. This situation is made worse by the fact that the government is increasingly collecting longitudinal data about students.[125] What should be done to improve education privacy?

[122] 20 U.S.C. § 1232g(a)(6). For criticism of the FERPA amendment, see Lynn M. Daggett, *FERPA in the Twenty-First Century: Failure To Effectively Regulate Privacy for All Students*, 58 Cath. U.L. Rev. 59, 100–01 (2008).
[123] 20 U.S.C. § 1232g(b)(2).
[124] 20 U.S.C. § 1232g(a).
[125] For a currently controversial proposal of the Department of Education to amend FERPA to permit greater collection of student information by the states, see Notice of Proposed Rulemaking, 76 Fed. Register 19726 (April 18, 2011). For a discussion of this proposal, see National Association of Independent Colleges and Universities, ED Proposes Regs to Reduce FERPA Privacy Protections (April 11, 2011), at http://www.naicu.edu/news_room/ed-proposes-regs-to-reduce-ferpa-privacy-protections.