Privacy 3.0--The Principle of Proportionality

Andrew B. Serwin
Individual concern over privacy has existed as long as humans have said or done things they do not wish others to know about. In their groundbreaking law review article The Right to Privacy, Warren and Brandeis posited that the common law should protect an individual's right to privacy under a right formulated as the right to be let alone - Privacy 1.0. As technology advanced and societal values also changed, a belief surfaced that the Warren and Brandeis formulation did not provide sufficient structure for the development of privacy laws. As such, a second theoretical construct of privacy, Privacy 2.0 as expressed in Dean Prosser's work Privacy was created. Dean Prosser continued (or expanded) upon the concepts formulated by Warren and Brandeis, particularly in emphasizing the role of common law in protecting privacy.

These works, while influential in their time, do not account for paradigm shifts in technology, or, perhaps more importantly, changes in how people live their lives. The unending advance of technology and changes in societal norms fundamentally dictate that privacy theory must change over time, or it will lose its relevance. Indeed, in today's Web 2.0 world where many people instantly share very private aspects of their lives, one can hardly imagine a privacy concept more foreign than the right to be let alone.

The question confronting modern-day privacy scholars is this: Can a common law based theory adequately address the shifting societal norms and rapid technological changes of today's Web 2.0 world where legislatures and government agencies, not courts, are more proactive on privacy protections?

This article argues that the answer is no and instead argues that the overarching principle of privacy of today should not be the right to be let alone, but rather the principle of proportionality. This is Privacy 3.0.
Privacy 3.0 – The Principle of Proportionality

By: Andrew B. Serwin
Privacy 3.0--The Principle of Proportionality

I. Introduction

Individual concern over privacy has existed as long as humans have said or done things they do not wish others to know about. While societies have had different formulations of privacy, largely based upon factors such as cultural values, societal need, and technology, privacy remains an age old issue.

Indeed, some of the earliest privacy restrictions were on “eavesdropping.” While we now conceptualize this issue as an electronic communication concern, before telephones existed people were concerned about others listening at the “eavesdrop” of their houses. This concern changed as technology evolved in the late 1800’s, and the law attempted to react to new technology. In their groundbreaking law review article “The Right to Privacy”, Warren and Brandeis posited that the law, specifically the common law, should protect an individual’s right to privacy. This law review article was in large part driven by a technological advance that created quite a stir, particularly in light of the media practices of the day—the instant camera. If the instant camera gave them pause, one wonders what they would think of a world defined by Facebook and Flickr.¹

While Warren and Brandeis are often credited with creating the right of privacy, they certainly did not do so.² What they did do, however, is provide the theoretical construct that helped shape the parameters of privacy protection in the United States. Ultimately, while serving on the Supreme Court, then Justice Brandeis had the opportunity to address another privacy issue raised by changes in technology—specifically whether there was a constitutional prohibition on wiretapping and the use of pen registers on telephones. While many now feel that government should have no right to wiretap citizens without a warrant, the Supreme Court initially found that since a third-party’s facilities (the phone company’s) were inherently part of the communication, no right of privacy existed in relation to telephone calls.³ Ironically, it was the dissent by Justice Brandeis in this case and his reiteration of the core right articulated in the Warren and Brandeis article that perhaps best illustrates the first theoretical construct of privacy—the concept that individuals had the “right to be let alone.”—Privacy 1.0.⁴

With the passage of time, courts adopted this right and used the common law to enforce it. Moreover, as technology continued to advance and societal values also changed, a belief surfaced that the Warren and Brandeis formulation did not provide sufficient structure for the

¹ For the non-Web 2.0 readers, Facebook is the leading online social networking site, and Flickr is an Internet service that permits one to upload, tag and share photographs.

² For a detailed discussion of the origins and the substantial body of privacy law that predated Warren and Brandeis’ article, see Neil M. Richards and Daniel J. Solove, Privacy’s Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123 (2007).


development of privacy laws. As such, a second theoretical construct of privacy—Privacy 2.0 as expressed in Dean Prosser’s work “Privacy”—was created, and ultimately codified in the Restatement (Second) Torts. Dean Prosser continued (or expanded) upon the concepts formulated by Warren and Brandeis, particularly in emphasizing the role of common law in protecting privacy. Dean Prosser analyzed the flood of cases that flowed from the Warren and Brandeis article and categorized the privacy protections created by the common law into 4 distinct acts that were found to be violations of an individual’s right of privacy. While important, Prosser’s theory is one that is limited because its basis, like that of Privacy 1.0, is common law and tort.

These works, while influential in their time, do not account for changes in values, paradigm shifts in technology, or, perhaps more importantly, changes in how people live their lives. The unending advance of technology and changes in societal norms fundamentally dictate that privacy theory and its associated concepts must change over time, or they will lose their relevance.

A perfect example of the differences in our society can be seen by examining an issue that must be addressed by today’s privacy theory—health care record interoperability. Many states, including California, are requiring that health care entities that receive state funds become compliant with systems by 2014 that permit the sharing of medical information electronically. While setting the technological standards is a difficult task, setting the standards for privacy and security will present more complex challenges. In the time of Warren and Brandeis, a “right to be let alone” was a viable theoretical construct. In today’s society, information sharing here to stay, and privacy theory must adjust to meet this challenge. Indeed, in today’s Web 2.0 world where many people instantly share very private aspects of their lives, one can hardly imagine a privacy concept more foreign than the right to be let alone.6

Indeed, this is a point that can hardly be debated, since many modern scholars recognize that the prior theoretical constructs of privacy have not met the needs of individuals.7 This is ironic because despite the proliferation of privacy laws in the United States, more and more people feel they have less protection for their personal information.8 That the European Union (“EU”) found


6 This is not to say that everyone shares these values, or wants instant information sharing, but that truly is the point of Privacy 3.0, the principle of proportionality advocated by this article. While Privacy 3.0 has the flexibility to account for different viewpoints on the sharing of sensitive information, a theoretical construct as absolute as the “right to be let alone” does not have the same level of flexibility. While one can argue that an individual can choose, or not choose, to be let alone, today’s society functions on information sharing that many people take for granted. If one questions this premise, one need simply ask how many consumers have voluntarily placed a security freeze on their credit report if they have no reason to fear identity theft. While some may have done so, the vast majority have not, despite the availability of the right, because there is a societal benefit—readily available credit—that they enjoy as a result. Thus, we must recognize that absolute principles are not the appropriate model for information privacy in the United States.

7 Erwin Chemerinsky, Rediscovering Brandeis’s Right to Privacy, 45 Brandeis L.J. 643 (2007); Richards and Solove, supra note 2.

8 Indeed, Dean Chemerinsky recently noted that informational privacy “is the area of privacy law that is in the most dramatic need of development. There needs to be judicial protection of a constitutional right to
that United States’ law failed to adequately protect individuals’ privacy, and therefore banned the export of information regarding EU residents to the United States, only further illustrates this point.9

Some modern scholars characterize the issue as the need to continue the path of Warren and Brandeis, and have called on the courts to step in and constitutionally protect informational privacy.10 Other modern scholars have begun to question the path of Privacy 1.0 and 2.0 because both rest upon a theory of “inviolate personality.”11 These scholars have contrasted the Warren and Brandeis theoretical formulation of privacy with other common law decisions from England that rely upon a different theory—one based upon confidentiality—and posit that Warren and Brandeis followed the wrong path and instead should have used the confidentiality cases as their theoretical foundation.12

This article argues that questioning the assumptions of prior privacy theory is correct, and indeed necessary, at this time, but the questions that must be raised should not result in further use of theories that rely upon the common law. Indeed, further reliance upon common law, whether based upon “inviolate personality” or confidentiality, is not the correct solution and will not solve the underlying issue with common law based theories, because of the inherent limitations of tort law in the privacy context.

The question confronting modern-day privacy scholars is this: Can a common law based theory adequately address the shifting societal norms and rapid technological changes of today’s Web 2.0 world where legislatures and government agencies, not courts, are more proactive on privacy protections?

This article argues that the answer is no and instead argues that the common law based prior scholarship, was relevant for its day, it cannot account for: the technology and societal values of today; our statutorily-driven privacy protections; as well as a Federal Trade Commission-enforcement centric model, and should therefore not provide the theoretical construct for existing or future laws or court decisions. Indeed, this is all the more true in light of recent FTC guidance regarding behavioral advertising, in which the FTC expressly recognized the need to informational privacy and greater safeguards through tort law and statutes. The Supreme Court needs to recognize a fundamental right to informational privacy under the Due Process Clauses of the Fifth and Fourteenth Amendments. Tort law and statutes must do a better job of providing for liability for those who reveal deeply personal information about individuals. This is the unfinished legacy of Warren and Brandeis, and now, more than ever, it needs to be realized.” Chemerinsky, supra note 7, at 656-57.

9 In order to export most forms of data from the EU to the United States, companies must follow additional steps, including entering model contracts, complying with the Safe Harbor Program, or doing Binding Corporate Rules. For a complete discussion of these concepts, see, see Andrew Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, Chapter 26 (West 2007).

10 Chemerinsky, supra note 7, at 644-645.

11 Richards and Solove, supra note 2, at 127-130.

12 Richards and Solove, supra note 2, at 131-132
balance support for innovation and consumer protection, as well as the “benefits” provided to consumers by behavioral advertising.\textsuperscript{13}

The experience of the last 100 years, including the questions being raised today about the viability of prior theoretical constructs of privacy, demonstrates that common law theories that rely upon courts to drive doctrine are not the appropriate model where legislatures are more active in protecting privacy via statutes, and government enforcement mechanisms other than courts, particularly the FTC, are more likely to impact information privacy practices. But common law based theories face additional hurdles as well. Both Warren and Brandeis, as well as Prosser, explicitly rely upon tort enforcement for privacy violations.\textsuperscript{14} However, a model that relies upon tort enforcement is doomed to inconsistent results because relying upon tort enforcement ignores the reality that many privacy breaches that should give rise to a remedy of some sort, particularly in the case of truly sensitive information, do not because there is no “damage” suffered by the individual as a result of the breach. As discussed below, this has been an issue for courts, and will continue to be one as long as we rely upon common law models.

Moreover, reliance upon common law theories, even where the underlying theory is confidentiality, is not a viable option in today’s society because information sharing is core to our culture and society, and confidentiality as a theoretical construct is as limited as other common law based theories. Thus, a theoretical construct based upon the common law, particularly one that was created prior to the technological advances of today, provides little insight in the Web 2.0 world.

We find ourselves today in a situation where we have more privacy regulation than ever, yet we lack a relevant and cohesive theory of privacy. This failure leads to situations where individuals feel their privacy is not being protected, and people or entities that hold or process others’ data do not have clear guidance on proper information practices. As long as we rely on common law theories, no matter how many laws are passed, this will not change.\textsuperscript{15} All a common law based

\begin{flushright}

\textsuperscript{14} Warren and Brandeis explicitly state that tort enforcement is the appropriate mechanism to enforce privacy, as does Prosser, which is demonstrated by the adoption of his 4 categories of privacy violations into the Restatement (Second) Torts.

\textsuperscript{15} The pretexting issues that recently became news are a good example of this problem. While historically telephone connection records have not been entitled to extreme protections, public perception obviously was not in line with Supreme Court holdings, and there were those that believed that the practice of obtaining telephone records under false pretenses was already a crime, and California’s attorney general attempted to prosecute individuals for their alleged conduct. Simultaneously, many legislatures, including California, passed anti-pretexting laws to prohibit the conduct that purportedly was already criminal. In the end, a number of states passed anti-pretexting laws, and the Federal Communications Commission enacted a number of new regulations, and the charges were ultimately dropped. The principle and tiered system advocated by this article would provide more clarity than existing theories because once information is identified and placed in a tier, individuals and entities dealing with data will have a clearer picture of appropriate conduct and protections. See, Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, Chapters 4, 5, and 13 (West 2007)(discussing the law of pretexting and wiretapping).
\end{flushright}
model will ensure is that these laws will in many cases impose inconsistent burdens on information that will not meet the society’s need for privacy.\textsuperscript{16}

Given the changes in society, as well as the enforcement mechanisms that exist today, particularly given the Federal Trade Commission’s new focus on “unfairness,”\textsuperscript{16} and the well-recognized need to balance regulation and innovation, a different theoretical construct must be created—and it cannot be based upon precluding information sharing via common law methods. Instead, the overarching principle of privacy of today should not be the right to be let alone, but rather the principle of proportionality. This is Privacy 3.0.

The principle of proportionality recognizes that neither the government, nor private citizens, benefit (and indeed they have much to lose) from overbroad privacy restrictions.\textsuperscript{17} Indeed, overbroad privacy restrictions could jeopardize someone’s life if the sharing of medical information is hindered in an emergency situation. Other examples include purchasing necessary goods based upon easily available credit, and finding people with the same interests via a social networking site. This is not to say that information should be freely available and access should be granted to any petty thief who seeks to do harm. Instead, a theory of proportional protection places higher restrictions and access barriers on truly sensitive information that either has limited or no use to third-parties and has great capacity to damage individuals and society, while simultaneously permitting necessary and appropriate access to those having a legitimate need to know certain information, particularly when that information is less sensitive. Proportionality also has the advantage of minimizing the societal impact of privacy issues because enforcement and compliance will be focused on the most appropriate levels of sensitive information.

While the principle alone provides some guidance, it is the application of the principle of proportionality to create four tiers of information that is the most important aspect of this theory of privacy. While ultimately this model could be based upon a continuum, the use of a matrixed approach would cause the model to lose some of its predictive ability since the grouping of similar information into tiers facilitates more detailed guidance. Indeed, the four tiers will provide guidance on existing issues, attempt to bring cohesion to the numerous state and federal laws, as well as provide guidance for new issues and data types once they are characterized as falling within one of the tiers. Using pretexting as an example, once telephone records are placed in their appropriate category, understanding what conduct is appropriate and whether there is a specific law in place precluding the practice, becomes a much simpler and clearer task. More importantly, while the tiers provide much needed structure, the principle of proportionality ensures that the theoretical construct can easily deal with changes in technology. Using connection records (the subject of pretexting) as an example, as more as new methods of communication are created, by using the predictive nature of the tier methodology, one can attempt to predict how legislatures and courts will treat records related to new forms of communication, even before laws are in place.


\textsuperscript{17} As noted below, this concept is implicit in the FTC’s formulation of what is an “unfair” business practice, which is a now a common privacy and security enforcement theory.
Changes in societal norms and values can also be more easily addressed. As we have seen from the meteoric rise of the Internet and related technologies, new technology both creates new privacy concerns (via the creation of new forms of sensitive data), and renders certain privacy concerns related to older technology that is no longer used less relevant, therefore rendering the data less sensitive. The principle of proportionality, with its focus on the level of sensitivity of information, has the ability to account for those changes in a way that other models do not.

The need for a meaningful and relevant theoretical construct for privacy cannot be overstated. While statutes and cases ultimately set the standards for conduct, without the guidance provided by an appropriate theoretical construct for legislators, regulators, and courts on privacy issues, the result will be the continuation of inconsistent requirements that either are too restrictive, and therefore create economic and other barriers for society, or not restrictive enough to protect privacy, which also causes severe harm to individuals and society as a whole.

II. Privacy 1.0 - A historical background

While privacy was not invented by Warren and Brandeis, “The Right to Privacy” was, and is, the defining moment for privacy in the United States. Indeed, it is not an overstatement to say that their privacy theory was the foundation for privacy law in the United States, hence Privacy 1.0.

Warren and Brandeis were deeply concerned about the inability of the common law to protect an individual’s privacy, particularly due to advances in technology:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.\(^{18}\)

The technological advance that caused the most concern was the instant camera.\(^{19}\)

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone”. Instantaneous photographs and newspaper enterprise

---


19 This technological advance coincided with a paradigm shift in society—the increasing role of the media and in particular newspaper circulation. According to the research of Richards and Solove, the growth of the predominant media outlet of the time—newspapers—was astounding. In the 40 year period between 1850 and 1890 the number of newspapers grew from 100 to 900, with a corresponding increase in readers. Newspaper readers went from approximately 800,000 to more than 8 million people. Richards and Solove, *supra* note 2, at 128.
have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.”

... Of the desirability -- indeed of the necessity -- of some such protection, there can, it is believed, be no doubt. The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.20

While the problem was clearly identified by Warren and Brandeis, finding a legal theory that provided adequate protection proved more difficult.21 They first considered the law of defamation as a model for invasions of privacy. “Owing to the nature of the instruments by which privacy is invaded, the injury inflicted bears a superficial resemblance to the wrongs dealt with by the law of slander and of libel, while a legal remedy for such injury seems to involve the treatment of mere wounded feelings, as a substantive cause of action.” 22 However, the law of defamation was ultimately rejected because it was based upon a “radically different class” of damages to an individual.23 This was in part, because if the action was otherwise lawful, common law, unlike Roman law, it did not recognize a claim for mere mental injury.24

Warren and Brandeis then considered whether principles of contracts could be applied to protect privacy, noting that there was some basis in prior case law to conclude that they could. “It should be stated that, in some instances where protection has been afforded against wrongful publication, the jurisdiction has been asserted, not on the ground of property, or at least not wholly on that ground, but upon the ground of an alleged breach of an implied contract or of a

20 Warren & Brandeis, supra note 4, at 195-196.
21 “It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.”  Warren & Brandeis, supra note 4, at 193-194.
22 Warren & Brandeis, supra note 4, at 196.
23 “The principle on which the law of defamation rests, covers, however, a radically different class of effects from those for which attention is now asked. . . . the wrongs and correlative rights recognized by the law of slander and libel are in their nature material rather than spiritual.”  Warren & Brandeis, supra note 4, at 196.
24 Injury of feelings may indeed be taken account of in ascertaining the amount of damages when attending what is recognized as a legal injury; but our system, unlike the Roman law, does not afford a remedy even for mental suffering which results from mere contumely and insult, but from an intentional and unwarranted violation of the “honor” of another.  Warren & Brandeis, supra note 4, at 196.
trust or confidence.” Despite this, they ultimately rejected this theory, finding that a contractual theory was too narrow to address the privacy harms of the day.

Warren and Brandeis then concluded that the extension of the common law could address privacy concerns. They noted that “[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.” This right was seen as a broad right of privacy, against an individual, irrespective of privity of contract. This was based upon a belief in the “inviolate personality,” which was expressed in the oft-quoted formulation of privacy of the time—the “right to be let alone.” While Brandeis receives credit for inventing this right, as noted above, it was a phrase coined by Judge Thomas Cooley in a tort treatise. Warren and Brandeis explicitly relied upon common law theories, as well as common law enforcement. They saw actions for tort damages being a critical part of the enforcement of the right of privacy.

Richards and Solove question the use of the right to be let alone as a privacy concept. The concept was originally used by Judge Cooley in the context of a plaintiff who had suffered an assault where no physical contact occurred. In modern parlance, this would be an intentional

---

25 Warren & Brandeis, supra note 4, at 201.
26 "This process of implying a term in a contract, or of implying a trust (particularly where a contract is written, and where there is no established usage or custom), is nothing more nor less than a judicial declaration that public morality, private justice, and general convenience demand the recognition of such a rule, and that the publication under similar circumstances would be considered an intolerable abuse. So long as these circumstances happen to present a contract upon which such a term can be engrafted by the judicial mind, or to supply relations upon which a trust or confidence can be erected, there may be no objection to working out the desired protection though the doctrines of contract or of trust. But the court can hardly stop there. The narrower doctrine may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.” Warren & Brandeis, supra note 4, at 202.
27 Warren & Brandeis, supra note 4, at 197.
28 "We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect of or the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.” Warren & Brandeis, supra note 4, at 203.
29 Warren & Brandeis, supra note 4, at 200.
30 Richards & Solove, supra note 2, at 128.
31 Warren & Brandeis, supra note 4, at 200; “[t]he doctrines of contract and of trust are inadequate to support the required protection, and the law of tort must be resorted to. The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested.”
32 Richards & Solove, supra note 2, at 130.
infliction of emotional distress claim. Given the fundamentally different nature of infliction of emotional distress claims, and informational privacy issues, the questions raised by Richards and Solove seem quite appropriate.  

Despite its inapplicability to privacy, the right to be let alone became one of the enduring privacy concepts. Not only did it appear in “The Right to Privacy,” it also appeared in one of Justice Brandeis’ most famous dissents, in the *Olmstead* case.

> “[The makers of our Constitution] conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.” (Brandeis dissenting) *Olmstead v. U.S.*, 277 U.S. 438, 48 S.Ct. 564 (1928).

> “Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.” (Brandeis dissenting) *Olmstead v. U.S.*, 277 U.S. 438, 48 S.Ct. 564 (1928).

It should be noted that while Warren and Brandeis were the first to offer a cohesive privacy theory, these concepts were certainly implicit in the Bill of Rights, including in the Third and Fifth Amendment, as well as the Fourth Amendment’s restrictions on government searches and seizures. Moreover, as Richards and Solove correctly argue, there were a number of common law cases that had already recognized a right of privacy, albeit based upon a theory of confidentiality, or confidential relations.  

While Warren and Brandeis’s article was hailed and treated as the theoretical construct for privacy for over 100 years, recently modern scholars have begun to question its continuing viability. Richards and Solve, relying upon English common law, argue that Warren and Brandeis should have followed a different path—one that relies upon claims arising out of a “breach of confidence” instead of relying, as noted above, upon one that protects an “inviolate personality” from harm.

---

33 Richards & Solove, *supra* note 2, at 130. “Warren and Brandeis certainly found useful Cooley’s recognition of mental injury as a basis for tort recovery, but Cooley’s usage of “the right to be let alone” was fleeting and had no connection to privacy rights. By contrast, Cooley devoted an entire chapter of the same treatise to the law of “confidential relations,” but Warren and Brandeis did not discuss it.”

34 “The law of confidential relations applied to specific relationships such as those enumerated by Cooley in his treatise. Nevertheless, this list was insufficient to protect instances of disclosure of confidential information in other relationships. In this context, English courts of equity filled the gap by fashioning an action for breach of confidence that could apply even where there was no attorney-client relationship or other “direct confidential relation,” such as the disclosure of personal or trade secrets. Legal remedies for divulging such confidential information began to emerge as early as the eighteenth century.” Richards & Solove, *supra* note 2, at 136.

35 Richards & Solove, *supra* note 2, at 133. “Warren and Brandeis did not expressly reject breach of confidentiality as a remedy for invasions of privacy, but instead of developing this concept and line of cases, they shifted to a different path. They explained the goal of privacy protections not as enforcing the norms and morality of relationships but as protecting an “inviolate personality” and the feelings of the individual from injury.”
Moreover, ironically, given that the technological driver of Warren and Brandeis’s article was instant photography, a recent law review called for additional federal legislation to address the tagging and dissemination of photographs on the Internet, finding that traditional privacy laws, particularly tort-based theories, were not adequate to address this issue.36 While not directly questioning the Warren and Brandeis model, it is indeed notable that the very issue they wrote about still defies current privacy theory.

III. Privacy 2.0 - A historical background

While groundbreaking, Privacy 1.0 did not provide all of the structure needed by courts, particularly as technology advanced and concerns over privacy changed, which was noted by certain judges as well as Dean Prosser in 1960.37

Judge Biggs has described the present state of the law of privacy as “still that of a haystack in a hurricane.” Disarray there certainly is; but almost all of the confusion is due to a failure to separate and distinguish these four of invasions, and to realize that they call for different things.

Dean Prosser attempted to cure the disarray by creating the next theoretical construct of privacy - Privacy 2.0 -- and following a closely related path. In 1960 Dean Prosser examined a number of the cases that flowed from the Warren and Brandeis theory and categorized them into one of four categories, which ultimately served as the basis for the Restatement (Second) of Torts’ four categories of privacy torts: intrusion upon seclusion; appropriation of name or likeness; publicity given to private life; and publicity placing person in false light. While Dean Prosser’s goal was a noble one, the current commentary on privacy suggests that the hurricane is still blowing quite strongly.

The Restatement formulation of an intrusion upon seclusion finds liability where a person intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person.38 This claim consists solely of an intentional interference with a person’s interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.39 This theory tracks the Privacy 1.0 model quite closely.

36 “For several reasons, existing privacy law is simply ill-suited for this new invasion. First, traditional tort law does not recognize invasions of privacy that occur in public, such as the taking of a photo in any public location. Second, the few “public invasions” that do constitute torts involve celebrities or other individuals who have commercial interests in their likenesses. Third, courts have severely limited privacy protections in order to ensure that privacy claims do not limit the free flow of ideas.” In the Face of Danger: Facial Recognition and the Limits of Privacy Law, 120 Harv. L. Rev. 1870, 1872 (2007).

37 Prosser, supra note 5, at 407.

38 Restatement (Second) Torts, 652B.

39 Restatement (Second) Torts, 652B com a.
Appropriation of name or likeness exists when a person appropriates to his own use or benefit the name or likeness of another. Liability under the Restatement formulation can arise for publicity given to private life if one gives publicity to a matter concerning the private life of another, if the matter publicized is of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public. Both of these theories also track closely to the Privacy 1.0 analysis, though they are more focused on the imposition of liability. Finally, the Restatement imposes liability for publicity placing person in false light. This theory would seem to be encompassed in prior theory, though Prosser believed that the Warren and Brandeis did not deal with this directly.

IV. The Weaknesses of Common Law Theories

While the Prosser/Restatement model provides some additional framework to understand privacy concepts, it is still reliant upon common law, and still based in tort theory. Inherently this limits its usefulness in addressing the privacy issues of today. Indeed, one of the limitations of a common law/tort based model is at some level foreshadowed in the Warren and Brandeis article. When they were dismissing property law as a basis for the enforcement of privacy rights, they stated “where the value of the production is found not in the right to take profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right of property.” While this statement does not directly relate to the main issue faced by individuals in privacy enforcement today—the lack of damages as a result of privacy breaches—it is certainly a statement that demonstrates the difficulty tort-based theories face in addressing the privacy issues of a Web 2.0 world. Indeed, today there are numerous cases finding that tort liability does not exist in privacy cases, particularly those that arise from misuse electronic information, because there is no economic loss. Thus, courts today seem to be finding, like Warren and Brandeis noted about property claims, that liability cannot exist for “…the peace of mind or the relief afforded by the ability to prevent any publication at all…” at least where no economic loss has occurred.

As a result, both the Warren/Brandeis and Prosser theories of privacy have inherent weaknesses, particularly in an age of massive electronic databases, the Internet and communication via social networking. Moreover, given that the main risk to companies today for privacy issues is either government enforcement, or reputational harm that can destroy consumer confidence, an alternative to the common law/tort model must be examined. Concepts such as mitigation, while they exist in tort theory, place the burden on the victim of the wrongful act. In many of today’s privacy laws (such as HIPAA, and security breach notification laws), the obligation to mitigate harm falls on the person or entity that caused the harm, not the person that suffered the harm. Finally, as argued below, common law theory does not account for a number of the privacy

---

40 Restatement (Second) Torts, 652C.
41 Restatement (Second) Torts, 652D.
42 “There is little indication that Warren and Brandeis intended to direct their article at the fourth branch of the tort, the exploitation of attributes of the plaintiff’s identity.” Prosser, supra note 5, at 401.
43 Warren & Brandeis, supra note 4, at 193.
protections of our time, including “mitigation” type statues, as well as credit freeze laws and identity theft laws that restrict the misuse of information of deceased individuals.\footnote{It is hard to imagine a plaintiff less likely to bring a tort claim than a deceased victim of identity theft, though the social utility of having laws to prevent the misuse of personal information, whether it involves the leaving, or dead, cannot be questioned. However, concepts such as these are inherently inconsistent with common law concepts such as standing and damages.}

V. The Fall of Tort Theory

While, as demonstrated above, tort enforcement is the fundamental basis of Privacy 1.0 and 2.0, courts dealing with informational privacy have rejected tort recovery. The vast majority of these cases fail due to a perceived lack of damages.

In one of the first cases to reject an informational privacy claim due to a lack of damages, the Court in\textit{Trikas v. Universal Card Services Corp.}, 351 F.Supp.2d 37 (E.D.N.Y. 2005), rejected a plaintiff’s claim for violation of FCRA. In\textit{Trikas}, the plaintiff brought an action based upon the assertion that an account erroneously remained open on his credit report. The plaintiff claimed that he suffered emotional distress because of this, even though it was admitted that no creditor actually saw or relied upon the erroneous information.\footnote{\textit{Trikas}, 351 F.Supp.2d at 45 (“Here too, however, Plaintiff has not presented sufficient evidence of damages to survive summary judgment.  Plaintiff testified that he was never turned down for any credit because of the Bank’s actions, and that he never even applied for any credit during the time his account remained erroneously open. Plaintiff admits that he has not suffered monetary damages: ‘It’s not a value that I suffered monetarily, as you could say it, a dollar value, because this is, like I said, it’s emotional, it’s stress, it’s burden.’”). For a complete discussion of these concepts and privacy litigation generally, see Andrew Serwin, \textit{Information Security and Privacy: A Practical Guide to Federal, State, and International Law}, Chapter 25 (West 2007).} Under the theory espoused by Warren and Brandeis, and modern scholars, liability should have attached. However, the Court dismissed the claim because the plaintiff could not prove damages that were caused by the alleged violation, and instead claimed to have suffered the very type of mental anguish discussed by Warren and Brandeis.

There have been several recent cases that have addressed the issue of whether the breach of a privacy policy can support litigation against the party that breached its policy. Courts have reached the conclusion that the mere breach of a privacy policy may not be sufficient to establish a claim for damages. In\textit{Dyer v. Northwest Airlines Corp.},\footnote{\textit{Dyer v. Northwest Airlines Corporations}, 334 F. Supp. 2d 1196, 1198 (D.N.D. 2004).} a group of plaintiffs sued Northwest Airlines for allegedly disclosing personal information gathered via the Web to certain government agencies in direct violation of Northwest Airlines’ posted privacy policy.\footnote{\textit{Dyer}, 334 F. Supp. 2d at 1198.} Northwest advanced two theories to defeat the plaintiffs’ claims. First, that its online policy was not a contract, but rather an aspirational policy, the violation of which did not give rise to contractual liability. Second, Northwest Airlines argued that even assuming that its act was a breach of a contract, the plaintiffs could not show any damage that resulted from the disclosure. The Court accepted both arguments and dismissed the plaintiffs’ claims, finding that there was
no breach of contract for several reasons, including a lack of damages.  

In Stollenwerk v. Tri-West Healthcare Alliance, the Arizona district court addressed issues related to causation and the speculative nature of damages arising out of privacy breaches, even where indisputably certain identity theft issues have occurred. Tri-West maintained personal information regarding a number of current and former members of the U.S. Military, as well as their dependents and had experienced security breaches where unauthorized personnel entered their facilities. The plaintiff alleged that despite this event, another breach occurred when hard drives were stolen from the same facility and these hard drives contained plaintiffs’ personal information. Certain of the plaintiffs did not suffer identity theft instances, but incurred costs in connection with obtaining certain reports regarding their credit, as well as identity theft insurance. One of the plaintiffs had six credit accounts opened under his name.

While the Court noted that identity theft issues could frequently result in damages other than purely pecuniary damages, this was insufficient to state a claim for negligence, even though psychological or emotional distress, inconvenience and harm to credit rating or reputation could occur. The plaintiffs attempted to analogize a privacy breach that could lead to increased chance of identity theft to toxic torts. The Court soundly rejected this argument. Moreover, even though one of the plaintiffs had experienced credit issues, the court held that there was insufficient evidence showing that it was caused by the theft of hard drives and dismissed his claim as well.

The Court in Forbes v. Wells Fargo Bank, N.A. reached a similar conclusion. In this case, the plaintiffs’ personal information was obtained due to a theft of computers that contained unencrypted customer information including names, addresses, social security numbers and account numbers. It again was undisputed that plaintiffs had expended time and money to monitor credit, but there was no indication that the information had been accessed or misused. The Court rejected the plaintiffs’ claim that they had suffered damage due to the time and money they had spent because the plaintiffs could only recover for loss of time in terms of earning capacity or wages. The Court therefore rejected both the breach of contract and negligence claim.

---


50 Stollenwerk, at *4.

51 Stollenwerk, 2005 WL 2465906 *4, (D.Ariz. Cpt. 6, 2005)(“The Court must acknowledge the important distinction between toxic tort and products liability cases, which necessarily and directly involve human health and safety, and credit monitoring cases, which do not.”) (internal citations omitted)

52 Stollenwerk, at *7.


54 Forbes, at 4; see also Cox v. Chicago Great Western R. Co., 176 Minn. 437, 223 N.W. 675, 677 (1929).
In *Bell v. Acxiom*, the Court addressed the issue of damages in a privacy case arising out of a computer hacking incident. The plaintiff alleged that the hacking incident compromised her personally identifiable information and that “lax security” left her at risk for privacy issues, as well as receiving junk mail.\(^{55}\) The main issue addressed was whether the plaintiff had standing to pursue the claim. Standing typically requires a showing of three requirements. The plaintiff must show: (1) that he has suffered injury in fact which is actual, concrete, and particularized; (2) a causal connection between the conduct complained of and the injury; and (3) that the injury will be redressed by a favorable decision.\(^{56}\) It should also be noted that the plaintiff has the burden of proof on these issues.\(^{57}\) Also, potential, future injuries do not constitute a sufficient showing by the plaintiff.\(^{58}\) In this case, because the plaintiff could not show injury, or even that she received any junk mail, the Court dismissed her case.\(^{59}\)

Similar conclusions have been reached by other courts, including in the *DSW* matter.\(^{60}\) The *DSW* case was recently followed by another court in Ohio.\(^{61}\) In this case, there was a security breach that could have resulted in the disclosure of the plaintiff’s personal information. The defendant advised all affected individuals to place a credit freeze on their report. Moreover, the plaintiff in this case could not establish any direct damages, other than costs associated with a credit monitoring service that the plaintiff purchased. The Court dismissed the claim, holding that any alleged damages were too speculative, particularly since the defendant had advised the plaintiff to place a security freeze on her credit report.\(^{62}\) The Court dismissed the claim despite the fact that the plaintiff was seeking reimbursement of monies paid for a credit monitoring service. In

---


\(^{58}\) *Bell v. Acxiom*, 2006 WL 2850042; citing *Sierra Club v. Robertson*, 28 F.3d 753 (8th Cir. 1994); *Whitmore*, 495 U.S. at 158.

\(^{59}\) Even if plaintiff had shown that she received junk mail, it is unlikely whether this would have been sufficient showing of injury. *Bell v. Acxiom*, 2006 WL 2850042, at *6. (holding that mere allegation of potential identity theft was insufficient to support the plaintiff’s claim); *Walters v. DHL Exp.*, 2006 WL 1314132 (C.D. Ill. 2006) (dismissing case based upon damage claim for increased risk of identity theft).

\(^{60}\) *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 688-69, 66 Fed. R. Serv. 3d 447 (S.D. Ohio 2006) (“Therefore, because the specific factual allegations of the Amended Complaint do not allege that the Plaintiff has personally experienced any injury other than ‘hav[ing] been subjected to a substantial increased risk of identity theft or other related financial crimes,’ the Court must accept the specific allegations Plaintiff makes as a true representation of the injury that the Plaintiff has suffered.”); citing *Courtney v. Smith*, 297 F.3d 455, 459, 2002 FED App. 0248P (6th Cir. 2002).


addition to this case, courts are still routinely finding that damages resulting from future identity theft are too speculative to be the basis of a successful civil claim.\cite{63} The lack of damage issue has also been addressed in the context of FCRA, at least for claims of actual damages.\cite{64} FCRA does, however, permit recovery of statutory damages, for willful violations, and claims without damages can in certain cases survive.\cite{65} This was also the conclusion of the Court in cases involving American Airlines and JetBlue.\cite{66}

The failings of tort theory also appear in cyber defamation cases, albeit due to the value judgment made by Congress to protect publishers of information on the Internet. The Communications Decency Act provides broad immunity to publishers on the Internet for postings by third-parties. While tort remedies can exist against the poster, there is no liability for the publisher, and perhaps more importantly, no obligation for the publisher to remove admittedly defamatory content.\cite{67} Thus, while a tort remedy might exist against the poster of the information, who in many cases is hard to identify and may not have sufficient assets to satisfy any judgment, the defamatory information still remains available and continues to cause damage.

While this is not to say that privacy tort claims do not succeed, this sampling of cases demonstrates that particularly for informational privacy concerns, a theory based upon tort law concepts has significant limitations, at least at this point in jurisprudence. This is particularly true since government enforcement is frequently the motivating factor for privacy compliance.

VI. The Rise of the FTC -- Current Enforcement Theories and Their Reliance Upon Proportionality

Proportionality is more consistent with the theoretical underpinnings of recent FTC enforcement actions than a common law based theory, particularly in light of the recent FTC behavioral advertising guidance.\cite{68} The FTC is the main privacy enforcement agency at the federal level, and truly sets the tone for privacy compliance in the United States, as is shown by the number of privacy and security enforcement actions brought by the FTC, as well as the record fines recently levied. Section 45 of the Federal Trade Commission Act, one of the main basis of the FTC’s enforcement power, makes “[u]nfair methods of competition in or affecting commerce, and

\begin{itemize}
  \item \textit{Schroeder v. Capitol Indemnity Corp.}, 2006 WL 2009053 (E.D. Wis. 2006) (granting summary judgment, in part, and dismissing portion of claim under FCRA because plaintiff failed to evidence of actual injury.)
  \item \textit{Schroeder v. Capitol Indemnity Corp.}, 2006 WL 2009053 (E.D. Wis. 2006); \textit{citing Murray v. GMAC Mortg. Corp.}, 434 F.3d 948 (7th Cir. 2006).
\end{itemize}
unfair or deceptive acts or practices in or affecting commerce” unlawful. While the deceptiveness prong of Section 45 was the more common enforcement mechanism, recent cases have increasingly relied upon the unfairness prong of the FTC Act.

While these cases are discussed below, the most recent guidance from the FTC, *Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles*, also recognizes the principle of proportionality. In this guidance the FTC recognizes the need to balance support for innovation with the need to protect consumers from harm. Moreover, the FTC also recognized the benefits that consumers derive from information sharing, including free information and services on the Internet. Finally, the FTC also noted that for purposes of data security, the sensitivity of the data is an important factor to weigh in assessing the needs and that while certain forms of data collected for behavioral advertising are sensitive, there are other forms that are not identifiable, and therefore less of an issue if wrongfully acquired. Both concepts are difficult for tort law to address, but they are inherently consistent with the principle of proportionality.

**In the Matter of Vision I Properties, LLC**

In the case of *In the Matter of Vision I Properties, LLC, d/b/a CartManager International*, the FTC started an investigation of a company that provided a shopping cart service for other e-commerce websites. These websites made specific representations regarding privacy, including that personal information was not sent, sold, or leased to third-parties. The FTC alleged that CartManager, a company that provided shopping cart services for these websites, violated the FTC Act. In most cases, the portions of the websites that gathered the information were CartManager’s, but CartManager did not disclose that the information practices on these pages were different from other pages, despite the fact that the pages appeared to be part of the same website. The FTC claimed that CartManager had also begun renting information to third-parties, despite the privacy statements made by the retailers. Furthermore, CartManager allegedly failed to disclose its information practices to its clients. The FTC considered these acts to be violations of the FTC Act. The consent order that was entered by CartManager restricted its ability to disclose personally identifiable information, required it to pay certain costs, required additional disclosures regarding CartManager’s privacy practices and placed it under reporting obligations to the FTC.

The importance of this enforcement action was that, unlike prior enforcement cases, there was no direct representation to consumers – a standard prerequisite for deceptive practices under Section

---


70 See *In the Matter of BJ’s Wholesale Club, Inc.*, in which the FTC alleged that the mere failure to secure credit card information, though there was no specific statutory requirement to do so, was an unfair business practice.


72 This matter involved a draft complaint that was not filed because the matter was resolved via consent order.
Moreover, at that point it remained unclear whether the FTC was relying upon a third-party beneficiary theory, or its ability to act against unfair business practices.

The FTC began clearly using its “unfairness” power in *In the Matter of BJ’s Wholesale Club, Inc.* This case represents a marked departure from prior FTC actions. BJ’s Wholesale Club operates a number of membership warehouse stores. As part of its normal business, BJ’s accepted credit cards as a form of payment from its members. BJ’s collected personally identifiable information from its customers to authorize their credit cards. It also used wireless technology, including WAPs (wireless access points) and scanners to monitor inventory. The FTC filed a complaint against BJ’s, alleging that it had: failed to encrypt information while it was in transit or stored on the network; stored personally identifiable information in a file format that permitted anonymous access; did not use readily accessible security measures to limit access; failed to employ sufficient measures to detect unauthorized access or conduct security investigations; and created unnecessary business risks by storing information after it had any use for the information, in violation of bank rules.

The FTC alleged that as a result of this conduct, millions of dollars in fraudulent purchases had been made. Though there was no federal statute that BJ’s conduct directly violated, the FTC concluded that these acts constituted an unfair business practice under the FTC Act and brought an enforcement action against BJ’s. In the past, the FTC had only acted in the security arena when a company was subject to heightened security burdens (under statutes such as HIPAA, COPPA, or GLB), or the company had made specific security promises. Here, however, the FTC showed that even in the absence of a specific representation or a statutory burden, companies can face enforcement action for a lack of information security based upon its “unfairness” authority.\(^\text{73}\)

The use of the unfairness doctrine by the FTC is consistent with the principle of proportionality. While the unfairness doctrine is an evolving one, the FTC did provide some guidance regarding what constitutes an unfair practice in a statement in 1980. The Commission stated that “[u]njustified consumer injury is the primary focus of the FTC Act”\(^\text{74}\) and also noted “that to justify a finding of unfairness, any consumer injury must satisfy three tests: (1) the injury must be substantial; (2) it must be not outweighed by any offsetting benefits to consumers or competition; and (3) the injury must be one that consumers could not reasonably have avoided.”\(^\text{75}\) The FTC also stated that, “[a]lthough public policy” has been listed “as a separate consideration, it is used most frequently by the Commission as a means of providing additional evidence on the degree of consumer injury caused by specific practices.”\(^\text{76}\)

---

\(^{73}\) While BJ’s was the first FTC enforcement action to directly rely upon this theory, the unfairness theory was put forth several years before by Commissioner Mozelle Thompson in a separate statement in the *In ReverseAuction.com, Inc.* matter. Commissioner Thompson asserted that the FTC had the ability to bring data security enforcement actions based upon the allegation that a lack of data security was an unfair practice.

\(^{74}\) See [http://www.ftc.gov/os/2003/06/dotcomment.htm](http://www.ftc.gov/os/2003/06/dotcomment.htm); citing *Unfairness Statement* at 2, 104 F.T.C. at 1073.

\(^{75}\) See [http://www.ftc.gov/os/2003/06/dotcomment.htm](http://www.ftc.gov/os/2003/06/dotcomment.htm); *Id.* at 1073-74.

\(^{76}\) See [http://www.ftc.gov/os/2003/06/dotcomment.htm](http://www.ftc.gov/os/2003/06/dotcomment.htm); *Id.* at 1075
The formulation of the FTC’s unfairness statement is important, particularly now that the FTC is using unfairness as a basis for enforcement actions. The FTC’s focus on the balancing of consumer injury against benefits to consumers or competition is an analysis inherently consistent with the principle of proportionality that underlies Privacy 3.0.

VII. The Importance of Principle Based Analysis

The inherent limitations of prior privacy principles, and the emergence of an FTC enforcement centric model in the United States, could lead one to conclude the principles are not needed. However, the importance of principles to the law of privacy cannot be overstated. The fact that so many legal scholars have tried to bring forth a viable theory, despite the prior hurdles, shows the need and the importance of a workable theoretical construct. Simply put, no one wants the haystack in the hurricane to continue. The importance of principles is also shown by the number of countries that have adopted principle-based approaches via statutes, as well as the organizations such as the Organisation for Economic Co-operation and Development (“OECD”) was one of the first organizations to promulgate privacy principles, via non-binding guidelines. Though the United States is a member of the OECD, it has not adopted these principles in any way. However, these principles form the theoretical framework for the European Union’s Data Directive, which created the privacy protections that exist in the EU today. The first principle of the OECD guidelines is the collection limitation principle. The OECD Guidelines call for limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.77 The second principle is the data quality principle, which requires that personal data also be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, be accurate, complete and kept up-to-date.78 The third principle is the purpose specification principle, which requires that the purpose for which personal data is collected be specified not later than at the time of data collection and that the subsequent use be limited to the fulfillment of these purposes or others that are not incompatible with those purposes and as are specified on each occasion of change of purpose.79 The OECD guidelines also suggest that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with this requirement except with the consent of the data subject, or by the authority of law.80

The fourth OECD principle is the security safeguards principle. Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.81 The fifth principle is the openness principle and the Guidelines suggest that there should be a general policy of openness about

77 Part 2, Section 7.
78 Part 2, Section 8.
79 Part 2, Section 9.
80 Part 2, Section 10(a) to (b).
81 Part 2, Section 11.
developments, practices and policies with respect to personal data. Additionally, readily available means should exist to establish the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller. The sixth principle is the individual participation principle. The Guidelines suggest that individuals should have the right to: obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; be given reasons if a request is denied, and to be able to challenge a denial; and challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

The seventh principle is the accountability principle, which suggests that a data controller should be accountable for complying with measures which give effect to these principles. The eighth and final principle is International application principle. The Guidelines encourage Member countries to consider the implications for other Member countries of domestic processing and re-export of personal data. Member countries were also encouraged to take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure. A Member country was also cautioned to refrain from restricting transborder flows of personal data between itself and another Member country except where the other country does not substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.

Not to be outdone, the Asia-Pacific Economic Cooperation (“APEC”), also adopted principles that have served as the basis for privacy legislation in the Pacific Rim. The principles adopted by APEC are similar to the OECD principles, and they are: preventing harm; notice; collection limitation; uses of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability.

These principles are important to note because they do demonstrate that principles can dramatically impact privacy legislation, since these serve as the theoretical construct of the EU

---

82 “Data controller” means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. Guidelines Governing the Protection of Privacy and Transborder Flows of Persona Data, Part 1, Section 1(a). Part 2, Section 12.

83 Part 2, Section 13(a) to (d).

84 Part 2, Section 14.

85 Part 3, Section 15.


87 Part 3, Section 16.

88 Part 3, Section 17.

89 See, Andrew Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, Chapter 1 (West 2007) for a complete discussion of these principles.
Data Directive. More importantly, since the OECD principles serve as the basis of the EU Data Directive, and as noted below are quite similar to the principles specifically adopted by England, they demonstrate that England did not use its own common law as the theoretical construct of its privacy law, but rather relied upon other principles.

VIII. English Common Law is Not the Answer

Some scholars have suggested that an alternative theory of English common law, based upon confidences, which was not considered by Warren and Brandeis is the answer. However, the law of confidences fails for three reasons. First, as argued above, common law theories based upon tort remedies have not faired well in the United States, and will continue to fail as long as the damage and standing issues exist. Second, our society, in contrast to the societal values of England at the time that the confidence cases were decided, values information sharing, albeit with appropriate limitations.

Third, the theory of confidences, as a matter of policy, has not been adopted even by the English as their overarching policy. While English common law is certainly important to consider, the reality is that England has not chosen to rely on common law privacy protections and instead has protected privacy in a more comprehensive way than through its common law—it has implemented the EU’s Data Directive. Perhaps more importantly, it did so via the adoption of a number of principles, that in no way relate to the common law theory of confidences. While England does not explicitly recognize proportionality, it, like the tiers created by the application of the principle of proportionality, draws distinctions between personal data\(^90\) and sensitive personal information.\(^91\)

The principles that were adopted by England are: fair and lawful processing; obtaining data for specified and lawful purposes; adequacy and relevance of data; accuracy; data retention; recognition of rights; security; and onward transfer.\(^92\) Nowhere in these principles is the concept of confidence. Thus, if we are to look for a principle to follow for United States law, it should not be a principle that was rejected, at least implicitly, by England when it adopted its main data protection law. While one could conclude that following the English model, based upon the principles adopted in its Data Protection Act, is the answer to United States privacy concerns, these principles have not, and likely will not, be adopted as a model of United States privacy protection, though they do impact United States companies in certain circumstances.

\(^90\) “Personal data” means data which relate to a living individual who can be identified-(a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Data Protection Act 1998, Part I, Section (1).

\(^91\) Notably “sensitive personal data” means personal data consisting of information as to-(a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labor Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. Data Protection Act 1998, Part I, Section (2).

\(^92\) Data Protection Act 1998.
IX. The U.S. Adoption of EU-like Principles

While the United States has not used EU principles to end the hurricane noted by Prosser, that is not to say that U.S. law excludes principles entirely. In order to solve the issue created by the EU finding that the United States’ privacy laws were deficient, and therefore precluding transfer of personal information to the United States, a compromise was struck between the Department of Commerce and the EU. This resulted in the creation of the Safe Harbor program. A United States company could certify that it complied with certain principles and then transfer data from the EU to the United States.⁹³ There are seven U.S. privacy principles, and they are:

**Notice.** Companies can be required to give individuals notice about the purpose for which private information was gathered, as well as how information collected by a company will be used. A company can also be required to provide users with information regarding how they can register complaints.

**Choice.** Companies can be required to give users the option of not disclosing their personal information to a third party and requesting that their information not be utilized for purposes other than those originally disclosed at the time of collection. For certain sensitive information, Companies must receive explicit permission from the user before the information is disclosed to third parties or used for purposes other than that for which it was originally collected.

**Onward Transfer.** Before a company discloses any information to a third party, it can be required to apply the above-referenced notice and choice principles.

**Access.** Companies typically are required to permit users to have access to their personal information. A company can also be required to afford users the opportunity to amend, delete or alter personal information when it is inaccurate.

**Security.** A bedrock principle of many privacy laws is information security. While absolute security is not required, a company can be required to take reasonable precautions to protect private information from misuse.

**Data Integrity.** Ensuring the accuracy and completeness of the data can also be required. One of the main principals is that private information collected by a company must be relevant to the purposes for which it was collected.

**Enforcement.** Companies can also be required to provide some enforcement mechanism to protect an individual’s privacy rights, including a reasonably affordable and accessible dispute-resolution system.

---

While these principles exist and there is clearly dissatisfaction with current privacy theories in the United States, these principles do not serve as the theoretical construct for privacy laws in the United States. While the Internet and electronic communications are world-wide technologies, it is notable that the United States has not adopted the principles that the vast majority of other developed nations have. One of the explanations for the failure to adopt the EU principles is differences in cultural norms regarding information sharing.

X. A Current Assessment of Societal Views in the United States on Information Sharing and Management

Currently, concerns over privacy in the United States relate less either to torts or concepts such as misuse of a name or publicity given to private life. In fact, nowadays many people actually seek out opportunities to publicize private aspects of their lives. Social networking, blogging, and relatively easy consumer credit all depend upon information sharing to function. Indeed, in our consumer credit driven culture, the information sharing that is the cornerstone of readily-available credit is critical to many, and at least a significant luxury to others. None of these concepts are exclusively based in the United States, but there is a reason why social networking sites started in the United States, and that is a more liberal view of information sharing than many other countries.

This is not to say that information sharing does not have a societal price—the more information that is available, particularly in a public forum, the greater the chance for misdeeds—but despite these well-known risks, the concern most people have today is not completely being “let alone” or imposing tort liability for misuse, but rather permitting (and even facilitating) the public of their personal information, while retaining some control over its use. That is not to say that individuals do not want privacy. In a very real sense people are in many ways as desirous of privacy as ever, but they want also to enjoy the benefits of increased information sharing. This is particularly true with the rise of computers as an information center. In one of the more colorful discussions of the issue, one Ninth Circuit Justice offered the following:

[F]or most people, their computers are their most private spaces. People commonly talk about the bedroom as a very private space, yet when they have parties, all the guests—including perfect strangers—are invited to toss their coats on the bed. But if one of those guests is caught exploring the host’s computer, that will be his last invitation.\[94\]

While this statement is undoubtedly true, that same computer owner may be posting extensive details about himself on a social networking site via that very same computer. In other words, the theoretical basis of today’s privacy construct should be proportional restrictions, not outright prohibitions. This concept is the underlying basis of Privacy 3.0.

\[94\] United States v. Gourde, 40 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J. dissenting).
XI. Privacy 3.0

Given the speed at which technology now moves, any new privacy theory would need to provide guidance to individuals or entities that collect or process data where the law has not yet caught up to practices. As noted above, a good example of the need for this type of model is the pretexting issues that arose in recent times. Moreover, the theory should provide a unifying principle to understand the numerous privacy laws that exist and that are being enacted at an increasing pace and be consistent with current enforcement theories and help align laws and doctrines that are inconsistent with this principle. This leads us to the next iteration of privacy—Privacy 3.0.

Rather than being focused on broad rights, such as the right to be let alone, or tort concepts that do not lend themselves to the age we live in, Privacy 3.0 is built upon one principle—the principle of proportionality. While this concept is of more relevance to this time period, it alone would not go far enough. In order to be complete, the principle of proportionality must be applied and used to create four tiers of personal information—highly sensitive information; sensitive information; slightly sensitive information; and non-sensitive information. The level of security and privacy associated with each tier varies according to the sensitivity of the information, as do the methods that can be used to collect, process and use information.

The advantage of the tiers created by the application of the principle of proportionality is the incorporation of a principle-based approach in a way that does not operate to stifle information sharing as some current principle-based approaches do, while simultaneously defining permissible and non-permissible actions based upon the tier within which the information falls, even in the absence of specific statutory guidance. Thus, even if the law regarding a particular form of information is unclear, or non-existent, a company seeking guidance in an uncharted area can assess its conduct by comparing what is permitted with other similar forms of information. This approach also provides clarity regarding the underpinnings of existing laws, and guidance regarding future laws that will be necessary as new forms of information, and information sharing become more ubiquitous.

Categories of information will be placed in the tiers based upon a number of factors. The nature of the information, including how much the information reveals about an individual or a business\(^95\) (e.g., predispositions, preferences, personality traits, or susceptibility to diseases), is a critical factor to consider. The level of impact caused by disclosure of the information, whether to an individual or society, is also factor that must be considered when placing a category of information into a tier. The social utility of sharing of information will also be considered, as will the actual location of the information, since information that is in the public domain, or in a third-party’s hands, is sometimes subject to reduced protection.\(^96\) Whether the information can be used to obtain or create other information (such as a Social Security number) is a further

\(^{95}\) One advantage of this model is that it can bring consistency to laws related to informational privacy, whether they impact businesses or individuals, where appropriate.

\(^{96}\) Considering the social utility of sharing information would include a risk benefit analysis that would weigh the harm from disclosure and the potential misuse that could follow from unauthorized access or use versus the individual and societal benefit that is actually achieved from sharing information.
factor that effects the placement of information into a tier. The communication medium (including the form of the information) is also a factor to consider when examining the tier structure. Also, given the analysis utilized by courts in the Fourth Amendment cases, as well as trade secret cases involving proprietary information, what steps the person or business took to protect the privacy of the information is also a critical factor.

Once the information is placed into a tier, one can determine how information can be collected and used, because the differences in how information is collected, processed, used and disposed of all flows from the tier within which the category of information falls. Thus, there are common elements that will be discussed regarding each tier. These include:

- whether information can be gathered without notice or consent;
- whether consent must be opt-in or opt-out;
- the effect of consent;
- the types of processing that can be done;
- can information be gathered under false pretenses;
- are there time restrictions upon the retention of the data;
- data security requirements;
- data destruction requirements;
- what steps are required, or permitted, to mitigate any mishandling of information; and
- penalties for misuse of the information, including the imposition of statutory penalties in certain cases.

One introductory note regarding the creation of the tier system must be made at this point—while in the vast majority of cases governments have followed a similar path, and the protection afforded by the law is consistent, certain states or other government agencies have obviously not followed a uniform path in enacting laws. As such there will be laws, or portions of laws as noted below, that will be exceptions to the general categories described below. However, in many of these circumstances where legislation was enacted inconsistently with this model, courts have struggled with applying the law, particularly in situations such as the imposition of the interruption in service requirement under the Computer Fraud and Abuse Act.

A. Tier I-Highly Sensitive Information

---

97 Raskas v. Illinois, 439 U.S. 128, 152-153 (1978) (“The ultimate question, therefore, is whether one’s claim to privacy from government intrusion is reasonable in light of all the surrounding circumstances. . .”)(citations omitted).
Tier I information is information that is extremely sensitive\textsuperscript{98} and subject to strong limitations on collection, processing and disclosure, though in certain extremely limited cases the information can be collected and used without consent, particularly by the government. Examples of Tier I data would include genetic information, information regarding sexual history or other related issues, information related to religious affiliation, information regarding communicable diseases, many forms of health information, personal information regarding children under certain ages (particularly if it is gathered via the Internet), highly proprietary or confidential business information, or images or videotapes of conduct in private areas. While it remains to be seen, Radio Frequency Identification (“RFID”) may ultimately fall within this category, and despite the debate over Passenger Name Record (“PNR”), this information likely will fall within Tier I. Other forms of location tracking\textsuperscript{99} would also fall within Tier I.

Generally these types of information cannot be gathered without the express consent of the data subject, unless there is a truly compelling governmental purpose. For example, government agencies can collect DNA of people that have been convicted of certain crimes and this information can be processed for a limited period of time in a DNA database known as CODIS, the purpose of which is to solve crimes. Additionally, other examples of non-consensual collection or processing of this type of information are the often mandatory disclosures to governmental agencies that health care providers are required to make regarding communicable diseases.

However, if consent is given, processing and use is permitted, but it must be quite limited. Moreover, there frequently are time restrictions on the retention of the information as well as requirements of high levels of data security. Typically violation of these type of laws gives rise to severe civil, or even criminal sanctions.

\textsuperscript{98} While there can be subjective disagreement about what information is, or is not, extremely sensitive, in most cases there will be agreement regarding the categorization. Factors such as personal circumstances can impact someone’s subjective belief about sensitivity, but the categorization of information into Tiers would in many cases have to depend upon what society defines as sensitive in an analysis that in certain ways might be similar to the Fourth Amendment analysis of reasonable expectations of privacy on computers for government searches. \textit{See, e.g.}, \textit{U.S. v. Ziegler}, 456 F.3d 1138 (9th Cir. 2006), as modified, 474 F.3d 1184 (9th Cir. 2007). This is not to say that the Fourth Amendment analysis provides all of the answers, but it might provide some guidance where there are divergent views.

\textsuperscript{99} The acquisition of location data has been a difficult issue for courts, because the installation of a pen register on a cellular telephone can permit location tracking data to be gathered. Courts have reached different conclusions about the level of proof needed to monitor such data. In one matter a magistrate judge rejected the government’s request to obtain cellular site data which would have permitted the government to track a suspect’s whereabouts. \textit{In the Matter of the Application of the United States of America for an order authorizing the installation and use of a pen register and caller identification system on telephone numbers and the production of real time cell site information}, Case No. 05-4486 JKB; but c.f., \textit{In re Application of the United States of America for an order for disclosure of telecommunication records and authorizing the use of a PIN register and trap and trace}, Case No. 05-Mag.1763(permitting the gathering of location tracking information); \textit{In re Application for Pen Register and Trap/Trace device with Cell Site Location Authority}, 396 F.Supp.2d 747 (S.D.Tex. 2005)(same). These cases all treat the information as Tier I data, whether they permit disclosures based upon national security or a warrant. \textit{See}, Andrew Serwin, \textit{Information Security and Privacy: A Practical Guide to Federal, State, and International Law}, § 5:63 (West 2007)
B. Tier II-Sensitive Information

Tier II information is information that is still quite sensitive, but does not rise to the same level of sensitivity as Tier I information. Examples of Tier II information include the content of wire or electronic communications (if gathered precisely at the time of the communication); certain forms of health information; information regarding video rental and television programming preferences; financial information; consumer’s purchasing preferences, if tied to their identity; and Social Security numbers, particularly when combined with the person’s name. Generally this information is gathered with consent of the data subject, but it can be gathered without consent as well, or at least in the majority of cases, with opt-in consent. Even if information can be gathered without notice or consent, typically there are restrictions upon gathering information under false pretenses, particularly if the information is to be used for a fraudulent purpose. Moreover, in many cases the mandatory public display of Tier II information is prohibited (as is shown by Social Security number laws).

There are fewer restrictions on the processing and use of Tier II information, but the processing must typically be related to a legitimate purpose. Moreover, the government has increased ability to get Tier II information, even without a warrant, as demonstrated by FISA and the Patriot Act. As is shown by financial identity theft laws, fraudulent uses are typically prohibited, even if information is gathered legally. There are typically time restrictions on keeping Tier II information, and such information must typically be destroyed after the entity holding the data no longer has a need for it. Data security is required, but the requirements for data security for Tier II are not as rigorous as for Tier I data. The main remedies for misuse of Tier II information are civil, though criminal remedies do exist. Also, given the sensitivity of Tier II information, as with Tier I information, in many cases liquidated, or statutory damages, are available even if actual damages cannot be proven.

C. Tier III-Slightly Sensitive Information

Tier III information is information that is personally identifiable, but it is not as private as Tier I and II. Moreover, to the extent the information is sensitive, it is information that is routed through a third-party, thus there is a decreased expectation of privacy. Examples of Tier III information include: connection records from telephone companies or ISPs (but not the content of the communications); financial information regarding consumer debts; information disclosed on an employer’s computer network; and images captured in a public space. Connection records from an ISP, including IP addresses of websites visited, as well as to/from addresses for email, have also been held, at least by the Ninth Circuit, not to be private, based upon a pen register analogy, so these records would appear to fall within the same tier. Typically this information

100 United States v. Forrester, 495 F.3d 1041 (9th Cir. 2007) ("Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account. We conclude that these surveillance techniques are constitutionally indistinguishable from the use of a pen register that the Court approved in Smith. . . . Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties.")
can be gathered without consent, and notice is typically not required. In virtually every case, the individual can try and stop improper processing, but in most cases non-abusive processing can occur without consent. The government typically has much more latitude to collect this type of information, at times without a warrant, as is shown by the more limited restrictions on pen registers (devices that disclose the numbers an individual called without disclosing the content of the communication). Tier III information typically cannot be gathered under false pretenses, particularly if the information is gathered with fraudulent intent, which is shown by the pretexting laws that have recently been enacted.

There are general restrictions on data retention and destruction, but the requirements are not as rigorous as Tier I and II, as typically only “reasonable” steps need to be taken to secure and destroy data. Enforcement is typically exclusively civil, though fraudulent uses can subject a person to criminal sanctions.

D. Tier IV-Non-Sensitive Information

Tier IV information is information that still is personally identifiable, but is not truly private. Examples of Tier IV information include: a person’s name; email address; telephone number; and address. Tier IV information can typically be gathered without consent, and if consent is needed, opt-out consent usually is all that is needed. While much of this information is public, fraudulently gathering the information, particularly gathering the information in a way that misidentifies the person requesting the information, if it is done to further other misconduct, is typically prohibited. There are few restrictions on processing, except that fraudulent acts and deception are not permitted. While some data retention and destruction concerns exist, there are typically not extensive requirements on this type of data. While criminal enforcement can exist in limited circumstances, such as when other fraudulent acts are undertaken using this type of information, typically only civil remedies exist for violations related to Tier IV information.

XII. Privacy 3.0-Laws That Validate the Principle of Proportionality

While common law has not followed the principle of proportionality, existing legislation has incorporated the concept into numerous statutory schemes. A sampling of statutes that track this principle, as well as the protection afforded by the classification of information into tiers follows.

A. The Computer Fraud and Abuse Act (“CFAA”)

The CFAA was enacted to address the increasing number of computer crimes that were not covered under existing law. Up until 1994, the CFAA only provided criminal penalties, but statutory amendments to the CFAA added civil remedies and these remedies can be used by companies to protect their network and recover damages for unauthorized access. The CFAA can apply in a variety of contexts. It can be relevant in cases where business competitors improperly engage in certain conduct, including “scraping” websites. It is becoming more of an issue when employees depart and use a network to send or obtain trade secret information. It

---

also, of course, applies in the more traditional settings, including those involving hacking and the release of worms, Trojan horses, or other malicious programs, as well as the misappropriation, or damage, of private information.

It is a criminal act under the CFAA for anyone to intentionally access a computer without authorization, or beyond the scope of any authority that has been granted, whether the computer is owned by the government or not, if the conduct involved an interstate or foreign communication. It is also a criminal act to knowingly, and with the intent to defraud, access a protected computer: (i) without authorization; or (ii) beyond the scope of any authorization, if the person furthers a fraud and an item of any value is obtained, if the value obtained is over $5,000 in any one year period. The wages of employees used to repair damage can be considered when a court considers the $5,000 requirement. It is also unlawful for a person to knowingly cause the transmission of a program, code or command that intentionally: (1) damages a protected computer; (2) accesses a protected computer and recklessly causes damage; or (3) accesses a protected computer without authorization and causes resulting damage.

While this law appears to be quite broad, it recognizes, and is consistent, with the principle of proportionality. In order to prevail in a CFAA case, the plaintiff must show damage that is different that the tort concept of damage. Instead, in order to prove damage, the harm must be one of the following types: aggregated damage that exceeds $5,000; potential modification or impairment of a medical diagnosis, examination, treatment or care of one or more persons; physical injury; a threat to public health or safety; or damage to a government computer that is used in furtherance of the administration of justice, national defense or national security.

Notably, the damage issue still exists with the CFAA. Consistent with the damage issue presented by tort claims, courts have held that only expenses, specifically any “natural and foreseeable” expenses are part of the damages amounts that can be considered, but neither damages for emotional distress, or punitive damages, are recoverable.

The CFAA is a law that predominantly deals with Tier I information, as the information involved must implicate national security, medical information, or information that can cause more than trivial harm. The level of restrictions on disclosure of sensitive information are quite high, and the level of penalties available for violation of this law are also quite high, since criminal penalties, as well as civil penalties exist, including fines, are available. The enforcement pattern

---

104 U.S. v. Middleton, 231 F.3d 1207 (9th Cir. 2000).
of cases, even on the civil side, are consistent with this conclusion since most involve medical information, or highly sensitive business information, such as trade secrets or other proprietary information.

B. California’s Invasion of Privacy Act

California’s concern over privacy led it to be one of the first states to enact an array of criminal statutes, the purpose of which was to protect individual privacy. The California legislature noted that advances in science and technology had already led to the development of new devices and techniques that permit monitoring and recording of private communications, and that the invasion of privacy resulting from the continual and increasing use of these devices and techniques had created a serious threat to the free exercise of personal liberties. California felt such a threat it could not be tolerated in a free and civilized society. \(^{108}\) Thus, the legislature passed the “Invasion of Privacy Act” in order to protect the right of privacy of the people of California. \(^{109}\)

These restrictions are found in California Penal Code Section 631, \textit{et seq}.

California precludes any person from intentionally tapping or making an unauthorized connection with a telegraph or telephone wire, line, cable, or instrument, or a person who willfully and without the consent of all parties to the communication, or in any unauthorized manner reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the message is in transit over a wire, line, or cable, or a message is being sent from or received at any place in the state. \(^{110}\) California has also made it a crime to eavesdrop or record a confidential communication. A confidential communication is one had in circumstances as may reasonably indicate that a party to the communication desires it to be confined to the parties thereto. \(^{111}\) This does not include any communication that is made at a public gathering or in any legislative, judicial, executive or administrative proceeding that is open to the public or any other circumstance in which the parties might reasonably expect that the communication would be overheard or recorded. \(^{112}\)

California’s law is an example of a law that regulates Tier II information, though there are other portions that deal with Tier I information. It precludes the interception or recording of the content of communications without the consent of both parties. Moreover, reflecting the lower level of protection afforded to stored communications, it does not require two-party consent for the disclosure of a stored communication. California law has been held to permit employers to monitor communications on their networks if they have a policy in place that discloses this


\(^{109}\) Cal. Penal Code §630.

\(^{110}\) Cal. Penal Code § 631.

\(^{111}\) Cal. Penal Code § 632(c).

\(^{112}\) See, e.g., Cal. Penal Code § 633.
practice.\textsuperscript{113} Given that this is a Tier II law, criminal penalties, as well as civil penalties, are available. In other portions of its Penal Code, California generally permits law enforcement to wiretap if a warrant is obtained, which is also consistent with this law covering Tier II information, since notice is not required to the target of the wiretap.

This law also contains Tier I restrictions. California has made it illegal for a person or entity to use an electronic tracking device to determine the location or movement of a person.\textsuperscript{114} Given the highly sensitive nature of this information, violation of this portion of the law is a crime.\textsuperscript{115} However, consistent with Tier I, the law does not apply to the lawful use of an electronic tracking device by a law enforcement agency, given the compelling need of law enforcement for this sensitive type of data.\textsuperscript{116}

\textbf{C. DNA and CODIS}

The United States government has established an index of DNA, that contains DNA information and analysis of certain types of offenders, as well as selected individuals. This system is known as the Combined DNA Index System, or CODIS.\textsuperscript{117} This index is maintained by the FBI and contains the DNA identification records of persons convicted of crimes, persons who have been charged in an indictment or information with a crime, and other persons DNA samples collected under applicable legal authorities.\textsuperscript{118} This law permits the Attorney General\textsuperscript{119} to collect DNA samples\textsuperscript{120} from individuals who are arrested, facing charges, or convicted or from non-United States persons who are detained under the authority of the United States.\textsuperscript{121} There are certain mandatory collection requirements, including that the Director of the Bureau of Prisons is required to collect a DNA sample from each individual in the custody of the Bureau of Prisons who is, or has been, convicted of a qualifying Federal offense or a qualifying military offense. Additionally, the probation office responsible for the supervision under Federal law of an individual on probation, parole, or supervised release must collect a DNA sample from each individual who is, or has been, convicted of a qualifying Federal offense or a qualifying military offense.\textsuperscript{122}

\textsuperscript{113} One California court permitted e-mail monitoring of employees where the employee had agreed to a monitoring policy as part of an employee handbook. \textit{TBG Ins. Services Corp. v. Superior Court}, 96 Cal. App. 4th 443, (2002).

\textsuperscript{114} Cal. Penal Code § 637.7(a).

\textsuperscript{115} Cal. Penal Code § 637.7(e).

\textsuperscript{116} Cal. Penal Code § 637.7(c).

\textsuperscript{117} 42 U.S.C.A. § 14135a(a)(3).

\textsuperscript{118} 42 U.S.C.A. § 14132(a)(1)(A)-(C).

\textsuperscript{119} This authority can be delegated to the Department of Justice, and other agencies that arrest, detain or supervises individuals facing charges.

\textsuperscript{120} The term “DNA sample” means a tissue, fluid, or other bodily sample of an individual on which a DNA analysis can be carried out. 42 U.S.C.A. § 14135a(c)(1).

\textsuperscript{121} 42 U.S.C.A. § 14135a(a)(1)(A).

\textsuperscript{122} 42 U.S.C.A. § 14135a(a)(2).
This law governs Tier I data, so while there are certain governmental rights to obtain this data, for truly compelling purposes, there are restrictions on the collection and retention of the information. First, there are quality checks put in to ensure accuracy since CODIS can only include information on DNA identification records and DNA analyses that are based on analyses performed by or on behalf of a criminal justice agency or the Secretary of Defense in accordance with 10 U.S.C.A. § 1565 and in accordance with publicly available standards that satisfy or exceed the guidelines for a quality assurance program for DNA analysis, issued by the Director of the Federal Bureau of Investigation under 42 U.S.C.A. § 14131, or prepared by laboratories that: by October 30, 2006, have been accredited by a nonprofit professional association of persons actively involved in forensic science that is nationally recognized within the forensic science community; and undergo external audits, not less than once every 2 years, that demonstrate compliance with standards established by the Director of the Federal Bureau of Investigation.123

There are also specific privacy requirements, given the Tier I status of this information, including that the results of DNA tests performed for a Federal law enforcement agency for law enforcement purposes may be disclosed only: to criminal justice agencies for law enforcement identification purposes; in judicial proceedings, if otherwise admissible pursuant to applicable statues or rules; and for criminal defense purposes, to a defendant, who must have access to samples and analyses performed in connection with the case in which such defendant is charged.124

There are also expungement requirements that require the FBI to promptly expunge the DNA analysis of a person in two circumstances. If the original placement in the index was based upon a conviction for a qualifying Federal offense or a qualifying District of Columbia offense, the Director must expunge the record if he Director receives, for each conviction of the person of a qualifying offense, a certified copy of a final court order establishing that the conviction has been overturned.125 If the original placement was due to an arrest under the authority of the United States, the Director must expunge the record if the Attorney General receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.126 These requirements demonstrate the highly sensitive nature of this information, and the characterization of this law as a law covering Tier I information. In addition, there are criminal penalties for violation of this law.127

---

126 A court order is not “final” if time remains for an appeal or application for discretionary review with respect to the order. 42 U.S.C.A. § 14132(d)(1)(C).
128 42 U.S.C.A. § 14135a(a)(5).
D. Other Restrictions on Genetic Privacy

Alaska is one of many states that has placed strong restrictions on genetic privacy. It is generally illegal for a person to collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis unless the person has first obtained the informed and written consent of the person, or the person’s legal guardian or authorized representative, for the collection, analysis, retention, or disclosure. This restriction does not apply to DNA samples collected and analyses conducted for: certain limited statutorily defined purposes; a law enforcement purpose, including the identification of perpetrators and the investigation of crimes and the identification of missing or unidentified persons or deceased individuals; determining paternity; to screen newborns as required by state or federal law; or the purpose of emergency medical treatment.

Alaska law also provides that a DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled or analyzed. Given the concerns over this type of data, Alaska has specifically provided that a general authorization for the release of medical records or medical information may not be construed as the informed and written consent required by this law. There are civil penalties for violation of this law. Given the damage issues in privacy claims, the Alaska legislature provided for statutory damages for violations. In addition to the actual damages suffered by the person, a person violating this law is liable to the person for damages in the amount of $5,000 or, if the violation resulted in profit or monetary gain to the violator, $100,000. The law also provides for criminal penalties.

This is another example of law that covers Tier I information. As with the law that created CODIS, this law has quite strict restrictions on collection and disclosure of genetic information, even going to the point of granting the data subject an ownership right in the DNA material, and the test results. While there are exceptions that permit disclosure, they are quite limited.

---

129 “DNA” means deoxyribonucleic acid, including mitochondrial DNA, complementary DNA, and DNA derived from ribonucleic acid. Alaska Stat. § 18.13.100(1).

130 “DNA analysis” means DNA or genetic typing and testing to determine the presence or absence of genetic characteristics in an individual, including tests of nucleic acids or chromosomes in order to diagnose or identify a genetic characteristic; “DNA analysis” does not include a routine physical measurement, a test for drugs, alcohol, cholesterol, or the human immunodeficiency virus, a chemical, blood, or urine analysis, or any other diagnostic test that is widely accepted and in use in clinical practice. Alaska Stat. § 18.13.100(2).


134 Alaska Stat. § 18.13.010(c).


136 A person commits the crime of unlawful DNA collection, analysis, retention, or disclosure if the person knowingly collects a DNA sample from a person, performs a DNA analysis on a sample, retains a DNA sample or the results of a DNA analysis, or discloses the results of a DNA analysis in violation of this law. Alaska Stat. § 18.13.030(a).
Moreover, Alaska made clear that a general medical authorization does not grant a right to run DNA tests. Consistent with the Tier I nature of the information, criminal penalties exist for violations of this law. Finally, certain other states have even gone further, and limited the testing of relatives, as well as the data subject, to find genetic predispositions.137

E. Notice of Security Breach Laws

Notice of security breach laws have now swept the nation, with 39 states, and the City of New York, all enacting laws that require notice if there is a breach of security involving personal information of certain types.138 Many states have restricted notice to situations where there is unencrypted data at issue, but this is not always the case. Moreover, consistent with the tiered approach to privacy protection, only certain breaches of security—those involving truly sensitive forms of information require notice to consumers.

These laws are seen as quite critical to protecting individual privacy in the United States, though they appear to be inconsistent with the common law and tort based approaches of prior scholarship. This is for two reasons. First, while there certainly are breaches that cause consumers damages, the vast majority do not. While there are some states that do not require notice of breaches that are not reasonably likely to harm consumers, the vast majority of states have not adopted this standard. Second, these statutes impose liability for failure to give notice irrespective of damage to consumers. Thus, the tort concept of damages, and the inherent issues that it creates for privacy claims, was avoided because a different model based upon enforcement related to the sensitivity of the data was adopted.

California was the first state to require notice of data security incidents by enacting Civil Code Section 1798.82, which became effective July 1, 2003. As has been shown by the number of data security incidents that have been disclosed, this law has had a major impact on California companies, as well as any company that conducts business in California, whether headquartered in California or not.

Section 1798.82 is triggered if there is a breach of security and a consumer’s personal information is involved.139 Personal information was originally defined by the statute as either an individual’s first name or middle initial combined with a last name, and: a Social Security number; a California Driver’s License number or Identification Card number; or an account number or credit or debit card number and the Personal Identification Number (PIN), security code or password that would permit access to the account.140 However, recognizing the inherent sensitivity of other Tier I information, California recently amended the definition to include

---

137 See, e.g., Idaho Code Ann. § 39-8303(1)(a)-(d).
138 For a complete discussion of these laws, see, Andrew Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, Chapter 20 (West 2007).
140 Cal. Civ. Code § 1798.82(e).
“medical information\textsuperscript{141}” as well as health insurance information. Thus breaches involving this type of information must now also be disclosed under this law.

If the data owner reasonably believes that there has been a breach, Section 1798.82 mandates two different disclosures.\textsuperscript{142,143} The first, and most burdensome, is applicable if a person or business: conducts business in California; owns or licenses unencrypted computer data; and the computer data contains “personal information” regarding a resident of California. If there is a security breach of a computerized system that contains “personal information,” and it is known or reasonably believed that personal information has been acquired by an unauthorized individual, then the data owner must make a disclosure of the security breach to the affected California residents. While certain terms are defined by the statute, “acquisition” of information is not.

Notably, while not all states mandate notice unless there is a reasonable likelihood of harm (though California does not follow this model), violation of these laws typically subjects the person or company violating the law to civil sanctions, irrespective of whether there is damage or not.

Security breach laws are examples of laws that covers both Tier I and II information. In California’s case, it covers Tier I and II information since it requires notice for breaches involving Social Security numbers, health information, and financial account information if combined with other information that renders it capable of being exploited by an identity thief, and it does not depend on whether there is a likelihood of harm. In other cases where the security breach laws have broader definitions of personally identifiable information, other states have permitted companies not to give notice unless there is a reasonable likelihood of harm, which is consistent with the distinctions made between Tier I and II. One thing to note about these laws, which in essence require the party that has suffered a breach to mitigate the risks of the breach, the duty to mitigate is placed upon the party that would be a defendant in a civil suit, not the plaintiff, which is typically where the duty to mitigate is placed. While there are arguably tort concepts that would require the defendant in an action to take steps to mitigate harm, this again shows the inconsistency between general tort concepts, and privacy statutes we take for granted.\textsuperscript{144} Moreover, the form of information—computerized information versus information contained in other mediums that are not as likely to lead to massive identity theft—also impacts a company’s obligation to give notice, since under most laws only a breach

\textsuperscript{141} Medical information is defined as any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

\textsuperscript{142} Cal. Civ. Code § 1798.82(b).

\textsuperscript{143} Cal. Civ. Code § 1798.82(a)(b).

\textsuperscript{144} One other notable issue with notice of security breach laws is that they were generally adopted by the United States ahead of other countries, though this may just demonstrate that the United States information security laws generally lag behind other laws and therefore providing notice of breaches was necessary.
involving computerized data requires notice. This also is consistent with Privacy 3.0’s analysis.\textsuperscript{145}

\textbf{F. The Videotape Privacy Act}

The Videotape Privacy Act is a federal law that governs the disclosure of certain consumer video records and it, like the pretexting laws, resulted from a highly publicized privacy incident.\textsuperscript{146} It is a violation of federal law for any video tape service provider to knowingly disclose personally identifiable information\textsuperscript{147} concerning any consumer.\textsuperscript{148}

A video tape service provider can disclose personally identifiable information to the consumer, or to any person with the informed, written consent of the consumer given at the time the disclosure is sought. Disclosure can also be made to law enforcement agencies pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order.\textsuperscript{149}

A video tape service provider may also disclose the names and addresses of consumers if the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit disclosure and the disclosure does not identify the title, description, or subject matter of any video tapes. The subject matter of video tapes may be disclosed only if the disclosure is for the exclusive use of marketing goods and services directly to the consumer.

Disclosure is also permitted if the disclosure is incident to the ordinary course of business\textsuperscript{150} of the video tape service provider; or pursuant to a court order. Parties to a civil matter can obtain these records if they show a compelling need for the information that cannot be accommodated by any other means, if: the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.\textsuperscript{151}

\textsuperscript{145} One thing to note about these laws, which in essence require the party that has suffered a breach to mitigate the risks of the breach, the duty to mitigate is placed upon the party that would be a defendant in a civil suit, not the plaintiff, which is typically where the duty to mitigate is placed.

\textsuperscript{146} In this case a reporter sought and obtained Judge Bork’s video rental records during his confirmation hearings for the Supreme Court. This law was the result.

\textsuperscript{147} “Personally identifiable information” includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider. 18 U.S.C.A. § 2710(a)(3).


\textsuperscript{149} 18 U.S.C.A. § 2710(b)(2)(c).

\textsuperscript{150} “Ordinary course of business” means only debt collection activities, order fulfillment, request processing, and the transfer of ownership. 18 U.S.C.A. § 2710(a)(2).

\textsuperscript{151} 18 U.S.C.A. § 2710(b)(2).
If disclosure is authorized pursuant to a court order or a warrant the court is required to impose appropriate safeguards against unauthorized disclosure.\textsuperscript{152} Court orders authorizing disclosure to a federal or state agency can only be issued with prior notice to the consumer and only if the law enforcement agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry.\textsuperscript{153} If a State government asks for such records then the Court cannot issue the order if it is prohibited by state law.\textsuperscript{154} A court issuing an order may, if promptly requested by the video tape service provider, quash or modify the order if the information or records requested are unreasonably voluminous or if compliance with the order would otherwise cause an unreasonable burden on the provider.\textsuperscript{155} There are also data destruction requirements because video tape service providers are required to destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected, assuming there are no pending requests or orders for access to the information.\textsuperscript{156}

Injured plaintiffs are permitted to bring an action in the federal courts and may seek actual damages, but not less than liquidated damages in the amount of $2,500, punitive damages, reasonable attorneys’ fees and costs, and any other preliminary or equitable relief.\textsuperscript{157}

This law is an example of a law that covers Tier II information. There are quite broad restrictions on disclosure of video tape rental information, including notice to the consumer before a court orders disclosure, as well as data security requirements. Moreover, significant civil remedies are available, even in the absence of actual damages, which demonstrates the sensitive nature of the information, and illustrates again one of the failings of tort theory.

G. Federal Cable Privacy Act

In addition to the restrictions on video tape rental records, the federal government has also placed strict privacy restrictions on cable service providers. Cable service or other service\textsuperscript{158} providers must provide notice at the time of the entry of an agreement and at least once a year thereafter, in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of:

- the nature of personally identifiable information\textsuperscript{159} collected or to be collected with

\begin{itemize}
  \item \textsuperscript{152} 18 U.S.C.A. § 2710(b)(2).
  \item \textsuperscript{153} 18 U.S.C.A. § 2710(b)(3).
  \item \textsuperscript{154} 18 U.S.C.A. § 2710(b)(3).
  \item \textsuperscript{155} 18 U.S.C.A. § 2710(b)(3).
  \item \textsuperscript{156} 18 U.S.C.A. § 2710(e).
  \item \textsuperscript{157} 18 U.S.C.A. § 2710(c)(1) to (2).
  \item \textsuperscript{158} “Other service” includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; 47 U.S.C.A. § 551(a)(2)(B).
  \item \textsuperscript{159} “Personally identifiable information” does not include any record of aggregate data which does not identify particular persons. 47 U.S.C.A. § 551(a)(2)(A).
\end{itemize}
respect to the subscriber and the nature of the use of such information;

- the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

- the period during which such information will be maintained by the cable operator;

- the times and place at which the subscriber may have access to such information; and

- the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under this law to enforce such limitations.\(^\text{160}\)

Generally, a cable operator\(^\text{161}\) may not use a cable system to collect personally identifiable information concerning a subscriber without prior written or electronic consent.\(^\text{162}\) However, a cable operator may use the cable system to obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber, or to detect unauthorized reception of cable communications.\(^\text{163}\)

A cable operator cannot disclose a subscriber’s personally identifiable information without prior written or electronic consent. The cable operator must also take necessary actions to prevent unauthorized access to the information by persons other than the subscriber or cable operator.\(^\text{164}\)

A disclosure may be made if the disclosure is necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber. Disclosure of the names and addresses of subscribers to any cable service or other service, is permitted if the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and the disclosure does not reveal, directly or indirectly, the extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or the nature of any transaction made by the subscriber over the cable system of the cable operator. Disclosure to government entities is also permitted except that the disclosure cannot include records that reveal cable subscriber selection of video programming from a cable operator.\(^\text{165}\)


\(^{161}\) “Cable operator” includes, in addition to persons within the definition of cable operator in 47 U.S.C.A. § 522 of this title, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.


\(^{163}\) 47 U.S.C.A. § 551(b)(2).

\(^{164}\) 47 U.S.C.A. § 551(c)(1).

\(^{165}\) 47 U.S.C.A. § 551(c)(2).
There are also significant restrictions on the government’s ability to obtain this type of information. A governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if:

- the governmental entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

- the subject of the information is afforded the opportunity to appear and contest such entity’s claim.\(^{166}\)

There are also access and correction rights vested in subscribers. Cable subscribers must be provided access to all personally identifiable information that is collected and maintained by a cable operator. The information must be made available to the subscriber at reasonable times and at a convenient place designated by the cable operator. A cable subscriber must be provided reasonable opportunity to correct any error in such information.\(^{167}\)

There are also data destruction requirements in the Cable Privacy Act. A cable operator must destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access or pursuant to a court order.\(^{168}\)

Like many other Tier II laws, actual damages are available, as are liquidated and punitive damages, and attorneys’ fees.\(^{169}\)

This is another example of a law covering Tier II information. There are quite strong restrictions on disclosure, including the requirement that the subscriber be given notice before the government obtains information. There are also security and destruction requirements, as well as civil enforcement that includes liquidated damages. It should be noted that there are also a number of states that have enacted similar restrictions.

H. Credit Freeze Laws

Credit, or security freezes permit a consumer to place restrictions upon the use and disclosure of their consumer report.\(^{170}\) In many cases this is done after an incident that could lead to identity theft, or if identity theft is suspected. There are benefits to placing the freeze, but such action

\(^{166}\) 47 U.S.C.A. § 551(h).

\(^{167}\) 47 U.S.C.A. § 551(d).

\(^{168}\) 47 U.S.C.A. § 551(e).

\(^{169}\) Any effected person may bring an action in federal court seeking actual damages, or liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher, punitive damages, and reasonable attorneys’ fees and other litigation costs reasonably incurred. 47 U.S.C.A. § 551(f)(1) to (2).

\(^{170}\) For a discussion of credit freeze laws, see Andrew Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, Chapter 10 (West 2007).
also restricts the consumer’s ability to obtain credit, unless temporary lifts of the freeze are used. In certain states, insurers can deny insurance applications if the freeze is not lifted. Typically nominal fees can be charged for the placement, temporary lifts, or removal of the freezes.

These laws, which operate hand-in-glove with the notice of security breach statutes, because one of the main purposes of notice is to alert consumers so they can consider a credit freeze, or at least watch their credit report, are not consistent with common law concepts. In many cases (though there are exceptions) the consumer can place a freeze whether there is a risk of identity theft or not, thus obviating the need for any type of damage or causation elements, as tort theory requires. Moreover, as with the notice of security breach laws, there are statutory penalties, not just damages, that are recoverable for the violation of many of these laws. This model is inconsistent with traditional tort theory, with its requisite element of damages.

A good example of a comprehensive security freeze law is that of the state of New York. In New York, a consumer may request that a security freeze be placed on his or her consumer credit report by sending a request in writing by certified mail or by overnight mail to a consumer credit reporting agency at an address designated by the consumer credit reporting agency to receive such requests.

A consumer credit reporting agency that receives a written request from a consumer, as referenced above, must, if the written request is accompanied by proper identification and payment of any applicable fee, place a security freeze on the consumer’s consumer credit report

---

171 The term “security freeze” or “freeze” means a notice placed in the consumer credit report of or relating to a consumer, at the request of such consumer and subject to certain exceptions, that prohibits the consumer credit reporting agency from releasing the consumer credit report, the contents of such report or the credit score of such consumer. N.Y. Gen. Bus. Law § 380-a(m).

172 The term “consumer credit report” means a consumer report assembled, evaluated or maintained by a consumer credit reporting agency, bearing on a consumer’s credit worthiness, credit standing, or credit capacity. N.Y. Gen. Bus. Law § 380-a(l). The term “consumer report” means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or part for the purpose of serving as a factor in establishing the consumer’s eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) other purposes authorized under § 380-b of this article. The term “consumer report” does not include (i) any report containing information solely as to transactions or experiences between the consumer and the person making the report, (ii) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device, or (iii) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made and such person makes the disclosures to the consumer required under § 380-i of this article. N.Y. Gen. Bus. Law § 380-a(c)(1)-(2).

173 The term “consumer credit reporting agency” means a consumer reporting agency that regularly engages in the practice of assembling or evaluating and maintaining, for the purpose of furnishing consumer credit reports to third parties bearing on a consumer’s credit worthiness, credit standing, or credit capacity, public record information and credit account information from persons who furnish that information regularly and in the ordinary course of business. N.Y. Gen. Bus. Law § 380-a(k).

no later than five (5) business days after receiving the written request.\textsuperscript{175} If the written request is received after January 1, 2008, the consumer credit reporting agency must place a security freeze no later than four (4) business days after receiving the written request.\textsuperscript{176} The consumer credit reporting agency must send a written confirmation of the placement of a security freeze to the consumer within 10 business days of placing such freeze.\textsuperscript{177} After the freeze is placed, the consumer credit reporting agency must provide the consumer with a unique personal identification number or password, or other device to be used by the consumer when providing authorization for the release of his or her consumer credit report for a specific party or specific period of time.\textsuperscript{178}

If a consumer requests a security freeze, the consumer credit reporting agency must disclose the process of placing and temporarily lifting a freeze, and the process for allowing access to information from the consumer credit report for a specific party or a period of time while the freeze is in place.\textsuperscript{179}

If the consumer wishes to allow his consumer credit report to be accessed for a specific party or a specific period of time while a freeze is in place, he must contact the consumer credit reporting agency via certified mail, overnight mail, telephone or other method developed by the consumer credit reporting agency pursuant to the requirements below, and using a point of contact designated by the consumer credit reporting agency, request that the freeze be temporarily lifted, and provide: proper identification; the personal identification number or password provided by the consumer credit reporting agency; the proper information regarding the party to which the consumer credit report should be available or the time period for which the consumer credit report will be available to users of the report; and payment of any applicable fee.\textsuperscript{180} A request to temporarily lift a freeze must be complied with by the consumer credit reporting agency within three (3) business days after receipt of the request.\textsuperscript{181}

A consumer credit reporting agency can only remove or temporarily lift a freeze placed on the consumer credit report of or relating to a consumer: upon consumer request under this law; or if the consumer credit report of or relating to such consumer was frozen due to a material misrepresentation of fact by the consumer.\textsuperscript{182} If a consumer credit reporting agency intends to remove a freeze upon a consumer credit report pursuant to this latter exception, the consumer credit reporting agency must notify the consumer in writing prior to removing the freeze on such

\textsuperscript{175} N.Y. Gen. Bus. Law § 380-t(b).
\textsuperscript{176} N.Y. Gen. Bus. Law § 380-t(b).
\textsuperscript{177} N.Y. Gen. Bus. Law § 380-t(c).
\textsuperscript{178} N.Y. Gen. Bus. Law § 380-t(c).
\textsuperscript{179} N.Y. Gen. Bus. Law § 380-t(j).
\textsuperscript{180} N.Y. Gen. Bus. Law § 380-t(d)(1)-(4).
\textsuperscript{181} N.Y. Gen. Bus. Law § 380-t(e).
\textsuperscript{182} N.Y. Gen. Bus. Law § 380-t(h)(1)-(2).
consumer credit report.\textsuperscript{183}

This law does not apply to the use of a consumer credit report by: a person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account\textsuperscript{184} or collecting the financial obligation owing for the account, contract, or negotiable instrument; a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted for purposes of facilitating the extension of credit or other permissible use as well as certain exemptions for government actions.\textsuperscript{185} The other exemptions that are consistent with the societal values of the United States, as reflected in the principle of proportionality, including permitting transfers of information to facilitate certain financial transactions, particularly if there are suspicions of fraud.\textsuperscript{186}

This law is a law that covers Tier II information. While financial information is certainly sensitive, it does not receive the protection that other forms of information do. Here, a consumer’s information is shared, unless he or she “opts-out” of the sharing, and places a freeze, or hold, on disclosures of the information. Despite a consumer choosing to limit disclosures, there are still a number of circumstances where disclosure can happen, particularly if it relates to investigating fraud, or facilitating the collection of debts. Consistent with Tier II information, there are also procedures in this law to ensure accuracy of information.

I. Identity Theft

Identity theft laws are typically laws that cover Tier II information.\textsuperscript{187} These laws typically relate to reasonable sensitive information that is fraudulently used. They also have criminal and civil remedies available if a person violates these laws.

Delaware law provides a good example of identity theft laws. A person commits identity theft in

\footnotesize{\textsuperscript{183} N.Y. Gen. Bus. Law § 380-t(h)(2).}

\footnotesize{\textsuperscript{184} For purposes of this paragraph, “reviewing the account” includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.}

\footnotesize{\textsuperscript{185} N.Y. Gen. Bus. Law § 380-t(m)(1)-(8).}

\footnotesize{\textsuperscript{186} Certain entities are not required to place a security freeze on a consumer credit report, including: a check services or fraud prevention services company, which issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments; or a deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution. N.Y. Gen. Bus. Law § 380-t(p)(1)-(3).}

Delaware when the person knowingly or recklessly obtains, produces, possesses, uses, sells, gives or transfers personal identifying information\textsuperscript{188} belonging or pertaining to another person, without consent, and with intent to use the information to commit or facilitate any other crime.\textsuperscript{189} It is also a crime if the person knowingly or recklessly obtains, produces, possesses, uses, sells, gives or transfers personal identifying information belonging or pertaining to another person, without consent, thereby knowingly or recklessly facilitating the use of the information by a third person to commit or facilitate any other crime.\textsuperscript{190}

Identity theft in Delaware is felony. In addition to criminal remedies, a Court is also required to order restitution for monetary loss, including documented loss of wages and reasonable attorneys’ fees, suffered by the victim if a person is found guilty of identity theft.\textsuperscript{191}

Florida law also provides another example of an identity theft law that falls within the Privacy 3.0 framework. It is a crime in Florida for any person to willfully and without authorization fraudulently use, or possess with intent to fraudulently use an individual’s personal identification information\textsuperscript{192} without first obtaining that individual’s consent.\textsuperscript{193} This crime is a felony, punishable by a prison term of not greater than 5 years and a fine of not greater than $5,000, with additional penalties for habitual offenders, and higher levels of damages.\textsuperscript{194}

More importantly, Florida’s law demonstrates an inherent weakness of common law based theories with tort enforcement—misuse of deceased individual’s personally identifiable information. Florida has addressed this issue via statute and has made it a crime if any person

\textsuperscript{188} “Personal identifying information” includes name, address, birth date, Social Security number, driver’s license number, telephone number, financial services account number, savings account number, checking account number, credit card number, debit card number, identification document or false identification document, electronic identification number, educational record, health care record, financial record, credit record, employment record, e-mail address, computer system password, mother’s maiden name or similar personal number, record or information. Del. Code Ann. tit. 11 § 854(c).

\textsuperscript{189} Del. Code Ann. tit. 11 § 854(a).

\textsuperscript{190} Del. Code Ann. tit. 11 § 854(b).

\textsuperscript{191} Del. Code Ann. tit. 11 § 854(e).

\textsuperscript{192} “Personal identification information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any: 1. Name, postal or electronic mail address, telephone number, Social Security number, date of birth, mother’s maiden name, official state-issued or United States-issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card; 2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; 3. Unique electronic identification number, address, or routing code; 4. Medical records; 5. Telecommunication identifying information or access device; or 6. Other number or information that can be used to access a person’s financial resources. Fla. Stat. Ann. § 817.568(1)(f).


willfully and fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning a deceased individual commits the offense of fraudulent use or possession with intent to use personal identification information of a deceased individual.\textsuperscript{195}

J. Restrictions on Social Security Numbers

Social Security number laws provide another example of a Tier II law and Arizona’s law is discussed below.\textsuperscript{196} Arizona has made it illegal, as of January 1, 2005, for a person or entity to:

- Intentionally communicate or otherwise make an individual’s Social Security number available to the general public;
- Print an individual’s Social Security number on any card required for the individual to receive products or services provided by the person or entity;
- Require the transmission of an individual’s Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted;
- Require the use of an individual’s Social Security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the site; or
- Print a number that the person or entity knows to be an individual’s Social Security number on any materials that are mailed to the individual, unless state or federal law requires the Social Security number to be on the document to be mailed.\textsuperscript{197}

Arizona’s law does not prohibit the mailing of documents that include Social Security numbers sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the Social Security number.\textsuperscript{198} It also does not create an affirmative duty to inquire about the receipt of certain numbers from third-parties. A person or entity may print that number on materials that are mailed to the individual, unless the person or entity that received the number has actual knowledge that the number is or includes the individual’s Social Security number.\textsuperscript{199} This law also does not prohibit the use of a Social Security number if the use is continuous, and the person, after notice of the practice, does not object to the continued use.\textsuperscript{200} A person or entity that knowingly or intentionally violates Ariz. Rev. Stat. Ann. § 44-1373(A)(2), is subject to civil penalties.\textsuperscript{201}

\textsuperscript{196} see, Andrew Serwin, Information Security and Privacy: A Practical Guide to Federal, State, and International Law, Chapter 22 (West 2007) for a complete discussion of these laws.
This law is a law that covers Tier II information. Here, there are broad restrictions on the disclosure of Social Security numbers, but they are not absolute, particularly if there was a preexisting use. However, consistent with Tier II information, even with the preexisting use, the consumer can elect to stop that use if he or she objects. Given the sensitive nature of this information, and the possibility that damages cannot be proven as a result of the violation of this law, statutory penalties exist.

K. Pretexting

Pretexting laws, particularly those related to telephone records, are typically laws that fall within Tier III. Pretexting is an issue that caught the attention of regulators, in-house lawyers, and outside counsel in 2006. There are a number of laws that can regulate the practice of pretexting. A good working definition of pretexting is obtaining certain forms of information under false pretenses. Mainly this relates to the gathering of telephone records and financial information, though certain states, including Illinois, have expanded the definition of covered information. Illegal pretexting can be improper depending upon the type of data, the type of person seeking it, and the purpose of the request.

Pretexting is a complicated issue because the Supreme Court held that the right of privacy is limited in telephone connection records.202

The federal government enacted the Telephone Records and Privacy Protection Act of 2006, which governs pretexting.203 It is a crime for any person, in interstate or foreign commerce, to knowingly and intentionally obtain, or attempt to obtain, confidential phone record information204 of a covered entity205 by: making false or fraudulent statements or representations to an employee of a covered entity; making a false or fraudulent statements or representations to

---


204 The term used in the statute is technically confidential phone records information.

205 The term “confidential phone records information” means information that: (A) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer; (B) is made available to a covered entity solely by virtue of the relationship between that covered entity and the customer; or (C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer. 18 U.S.C.A. § 1039(h)(1).

206 The term “covered entity”: (A) has the same meaning given the term “telecommunications carrier” in section 3 of the Communications Act of 1934 (47 U.S.C.A. § 153); and (B) includes any provider of IP-enabled voice service. 18 U.S.C.A. § 1038(h)(2). The term “IP-enabled voice service” means the provision of real-time voice communications offered to the public, or such class of users as to be effectively available to the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, (whether part of a bundle of services or separately) with interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network. 18 U.S.C.A. § 1039(h)(4).
a customer of a covered entity; providing a document to a covered entity knowing that the document is false or fraudulent; or accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates 18 U.S.C.A. §1030 (the CFAA), without prior authorization from the customer to whom the confidential phone record information relates.\textsuperscript{207} It is also illegal to, unless otherwise permitted by law, knowingly and intentionally sell, transfer, or attempt to sell or transfer, confidential phone record information of a covered entity, without prior authorization from the customer to whom the confidential phone record information relates, or knowing or having reason to know the information was fraudulently obtained. This is also a crime, punishable by a fine, a prison term of not more than 10 years, or both.\textsuperscript{208} There are other additional restrictions in this law, as well as enhanced penalties and certain other limited exceptions.

This is a good example of a Tier III law. While there are criminal penalties involved, a violation of this law only occurs if the records were gathered in a fraudulent way, or other crimes are involved. Also, the law is somewhat limited because it only applies to the request, or receipt, of records from particular entities. Thus, while pretexting in many cases can be improper, the way the law treats the information, particularly in light of Supreme Court precedent, is consistent with Tier III.

L. CAN-SPAM

CAN-SPAM presents a clear example of a Tier IV law.\textsuperscript{209} CAN-SPAM, or Controlling The Assault of Non-Solicited Pornography and Marketing Act of 2003, was passed due to the legislative reaction to certain state e-mail laws, California’s in particular. These state laws went far beyond what the federal government was willing to do, so CAN-SPAM was passed with the goal of preempts (in essence nullifying) the troublesome portions of state law. CAN-SPAM was not a bill that was initially well received, though the criticism seems to have died down in recent times. The main criticism of CAN-SPAM is that it did not explicitly prohibit unsolicited e-mails. Despite this perceived shortcoming, CAN-SPAM has increased the FTC’s ability to stop spam. States at this point seem to be taking a back seat to the FTC on these issues, though state-based e-mail actions still occur.

Given the judgment by Congress that a person’s e-mail address did not justify the level of protection afforded by state law, CAN-SPAM in essence placed 3 main requirements on most entities that send e-mails. First, they must have a clear and conspicuous identification that the message is an advertisement or solicitation. Second, there must be clear and conspicuous notice of the opportunity to opt-out of future commercial e-mails, as well as the inclusion of a return address or other mechanism that allows opt-out requests.\textsuperscript{210} Third, each commercial e-mail must

\footnotesize
\begin{itemize}
  \item \textsuperscript{207} 18 U.S.C.A. § 1039(a).
  \item \textsuperscript{208} 18 U.S.C.A. § 1039(b)(1).
  \item \textsuperscript{210} 15 U.S.C.A. § 7704(a)(3)(a) to (b), (a)(5)(A) to (B).
\end{itemize}
contain a valid physical postal address for the sender.\textsuperscript{211} If affirmative consent from the recipient is obtained, then the clear and conspicuous statement that the email is an advertisement or solicitation is not needed.

There are of course other restrictions on emails under CAN-SPAM, including the adult-oriented rules, as well as criminal restrictions upon improper means of gathering email addresses, or misleading consumers, but there is no consumer redress for unsolicited email under CAN-SPAM.

This law deals with Tier IV information. Consumers can object to receiving emails, but it is not illegal for a person to send unsolicited emails. Moreover, the consumer at issue has no direct civil remedy for violation of this law. While there are criminal remedies in limited situations, these are only applicable if there is, in essence, independently improper conduct related to the use or gathering of addresses, or the registration of email addresses. Moreover, other remedies do exist, but they typically involve other deceptive conduct.

XIII. Legislatures Do Not Always Assess the Risks Correctly

The laws identified above that demonstrate the validity of Privacy 3.0 should not be read to mean that legislators always make the correct assessment. Indeed, one of the overarching needs to a viable theoretical construct is to provide guidance and a framework to make the laws more consistent. While there are certainly more than a few examples of laws that are inconsistent with the principle of proportionality, in many such cases courts and others have struggled with the application of these laws. One area where Congress did not more closely follow the factors arises from an amendment to the CFAA that occurred several years ago. In order to prove one type of claim under the CFAA the plaintiff must show “loss.”\textsuperscript{212} Previously there was no requirement that an electronic system be damaged, but the recent amendments added a new requirement—that there be some type of system interruption to show loss. This amendment does not truly capture the purpose of the law, and it adds a factor into the claim that does not truly matter in assessing whether conduct is wrongful. Indeed, if the information taken is highly sensitive, such as trade secrets, whether there was an impairment of the system or not would seem to be irrelevant to the harm inflicted by the conduct. Indeed, whether there is an interruption in service would be irrelevant under the Privacy 3.0 framework.

Courts have now struggled with this element of the CFAA. Courts in the Ninth Circuit continue to liberally permit claims under the CFAA where there is no clear allegation of system interruption, and therefore loss, as have other courts.\textsuperscript{213} However, many other courts have

\textsuperscript{212} 18 U.S.C.A. § 1030(a)(5).
\textsuperscript{213} See Therapeutic Research Faculty v. NBTY, 2:05-cv-2322-GEB-DAD (E.D.Cal. January 25, 2007)(holding that a claim could be stated under the CFAA against party that exceeded authorized use of password and thereby obtained additional access to licensed materials); citing Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F.Supp.2d 1121, 1126 (W.D.Wash. 2000); see also Sw. Airlines Co. v. Farechase, Inc., 318 F.Supp.2d 435, 439 (N.D.Tex. 2004); H&R Block E. Enter., Inc. v. J&M Secs., LLC, 2006 WL 1128744, at *4 (W.D.Mo. April 24, 2006); PharMerica, Inc. v. Arledge, 8:07-cv-00486-RAL-MAP (M.D.Fla. March 21,
struggled with this requirement and reached inconsistent results. The District Court in the Northern District of Indiana also recently assessed the damage element for a 1030(a)(5) claim in the context of alleged misconduct by an attorney as she departed her former employer. In Spangler, the defendant was a partner in a law firm and was alleged to have taken proprietary information, including client lists, and e-data files, before her departure for the firm, but as part of her plan to set up a competing law firm. The plaintiff moved for summary judgment on its CFAA claim. The Court ultimately denied the request, noting that while the plaintiff had alleged that it incurred costs to investigate the alleged improper access, it did not show that there was any impairment of data or the system, that supported a finding that the losses qualified as damage under 1030(a)(5). Again there are a cadre of other courts following this line of reasoning.

The interruption in service requirement continues to befuddle courts and two federal courts issued opinions on the issue within 2 days of each other, and reached opposite conclusions even though they relied upon the same cases to reach their respective conclusions. For example, in P.C. of Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, L.L.C., 2:04-cv-04554-JAG-MCA, some former employees allegedly took trade secret and confidential information regarding the plaintiff’s business and used it to open up competing businesses. The defendants brought a motion to dismiss the CFAA claim, asserting that the plaintiffs failed to state a claim under the CFAA, including because they had not demonstrated any “loss” under Section 1030(a)(5)(B)(1). The P.C. Yonkers Court examined the Nexans Wires case, as well as the Resdev case, and concluded that these cases made a distinction between costs incurred as a result of an incident, versus lost revenue or other consequential damages. The Court noted


215. Spangler, at 13; see also, Resdev, LLC v. Lot Builders Ass’n, 2005 U.S.Dist. LEXIS 19099 (D. Fla. 2005) (the CFAA requires some finding of “diminution in the completeness or usability of data or information on a computer system.”); Moulton v. VC3, 2000 U.S.Dist. LEXIS 19916, 20-21 (D. Ga. 2000) (investigative costs disallowed as damage under the CFAA where alleged incident did not result in “structural” damage to the network.).

216. Cenveo v. CelumSolutions Software GMBH & Co KG, 0:06-cv-0415-PAM-AJB (D.Minn. March 27, 2007)(dismissing CFAA claim based upon improper access to an employer’s confidential information because the complaint did not allege an interruption of service, and therefore failed to allege loss); see also Spangler, Jennings & Dougherty, P.C. v. Mysliwy, 2:05-cv-00108-JTM-APR (N.D.Ind. March 21, 2006)(allegations of downloading of firm information by attorney who was leaving her employer failed to demonstrate a CFAA because there was no allegation of system impairment, and therefore no loss).


218. The Court stated “As the Second Circuit found, ‘the plain language of the [CFAA] treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an ‘interruption in service.’” Nexans Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559, 562 (2d Cir. Feb. 13, 2006) (citing Civic Ctr. Motors, Ltd. v. Mason Street Import Cars, Ltd., 387 F.Supp.2d 378, 382 (S.D.N.Y. 2005) (ruling that loss of “competitive edge” claim not caused by computer impairment or computer damage was not cognizable under the CFAA); Resdev, LLC v. Lot Builders Ass’n, No. 04-Civ-1374, 2005 WL 1924743, at *5 (M.D. Fla. Aug. 10, 2005).
that loss under the CFAA is “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” The distinction the Court made is that in concluded that the “interruption of service” requirement applied only to the portion of the definition that addresses “any revenue lost, cost incurred, or other consequential damages”, but not to any allegation that related to “the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense . . .”. Thus, the Court read the definition of loss to have two different components, one of which does not require an interruption of service, if the loss relates to the costs of responding to an offense conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and a second component that includes lost revenue, incurred costs, or other consequential damages that result from an interruption of service. Under this definition, the Court concluded that the plaintiffs had stated a claim under the CFAA. What is notable, is that the plaintiffs in this matter never alleged there was either damage or an interruption of service, but rather that they had suffered “substantial losses in excess of $5,000, including but not limited to losses sustained in responding to defendants’ actions, investigating defendants; actions and taking remedial steps to prevent defendants’ further actions.” Nowhere did plaintiff articulate how it suffered damage to a computer or an interruption of service.

A different conclusion was reached in *L-3 Communications Westwood Corp. v. Robicharux*, 2:06-cv-00279-MLV-SS (E.D. La. March 8, 2007). In this case, former employees were alleged to have taken proprietary and trade secret information from their former employer, L-3, including via a number of emails that were sent, as well as an external drive that was used to copy an extensive number of confidential files. This information was allegedly used to compete with L-3 in an effort to obtain government contracts that L-3 was allegedly entitled to. This court relied upon the same cases that the *P.C. Yonkers* Court did, but reached a different conclusion. In fact, this Court created a two-pronged definition of loss, one portion of which requires damage to a computer, and one that requires an interruption of service and concluded that where the only allegation was theft of trade secrets and confidential information, and the resulting harm was

---

221 *P.C. of Yonkers, Inc.*, at * 8-10.
222 *P.C. of Yonkers, Inc.*, at * 9.
224 This Court concluded, based upon the *Nexans* case, that a plaintiff must allege either damage to a computer, or an interruption of service, to show loss under Section 1030(g). *L-3 Communications*, at *8, citing *Civil Center Motors, Ltd. v. Mason Street Import Cars, Ltd.*, 387 F.Supp.2d 378, 381 (S.D.N.Y. 2005) *Nexans*, 319 F.Supp.2d at 382 (“[C]osts not related to computer impairment or computer damages are not compensable under the CFAA.”)
misuse of the information to compete, without a showing of damage to a computer or an interruption of service, a CFAA claim could not be stated.\textsuperscript{225}

The confusion created by the insertion of the interruption in service requirement demonstrates the need for a cohesive theory of privacy based upon factors related to the sensitivity of the data, not whether a network was impaired. If the concern with the CFAA that led to the amendment inserting the interruption in service element was a concern that too many CFAA claims would be brought if the threshold was $5,000, then the dollar value of the information could be increased, or, following the tiered approach suggested in this article, it could be restricted to Tier I and II information over a certain value.

XIV. Conclusion

The failure of today’s privacy laws to meet societal needs can no longer be the subject of serious debate. The only question is should the common law serve as the basis for privacy theory in the United States. The inherent issues with common law theories resulting from today’s information sharing-based culture, the failure of tort theories to provide consistent enforcement, and the FTC enforcement centric model demonstrate the next theoretical construct of privacy should be the principle of proportionality, not the common law. Over time, the categories of information that fall within the resulting tiers will change, but the structure, and the general restrictions tied to each tier, will not. This will provide the stability necessary to bring order to the confusing morass of the privacy laws of today, and help guide the privacy laws of tomorrow.

Facebook and Flickr await.

\textsuperscript{1} Andrew Serwin is a partner in the San Diego office of Foley & Lardner LLP and specializes in information management matters. He has extensive experience in assisting companies with privacy and security issues, including state, federal and international restrictions on the use and transfer of information, security breach compliance, incident response, information management litigation, marketing restrictions, and the drafting and implementation of privacy and security policies, as well as broad experience in technology and business law, including corporate finance, partnership law, securities, e-commerce, software development and licensing, and intellectual property licensing and protection. He is the author of “\textit{Information Security and Privacy: A Practical Guide to Federal, State and International Law}”, a 2,000 page treatise on information security and privacy, and the “\textit{Internet Marketing Law Handbook}”, both published by Thomson-West. He has written over 50 articles, predominantly on information management and Internet issues, is also the author of the advertising section of the “\textit{ABA Model Web Site: A Knowledge Management Approach to E-Business Model Web Site}” that provides guidance on “best practices” for Internet issues, as well as Co-Chair and principle author of the Privacy and Security Section of the ABA’s publication, “\textit{Selling Products and Services and Licensing Software Online: An Interactive Guide With Legal Forms and Commentary to Privacy, Security and Consumer Law Issues}”, (June 2007).

He also serves on the privacy and legal subcommittees of the Privacy & Security Advisory Board of the California Health and Human Services Agency by the California Office of HIPAA Implementation, the Publications Board of the American Bar Association’s Business Law Section, and the editorial board of the Cyberspace Lawyer and the Privacy and Information Law Report. He is also the former Co-Chair of the California State Bar’s Cyberspace Law Committee.

\textsuperscript{225} \textit{L-3 Communications}, at *8.
The author would like to acknowledge Mark Foley, Chris Hoofnagle, James Kalyvas, Kristopher Keys, Peter McLaughlin, Michael Overly, and William Yoon for their valuable suggestions to this article.