University of Michigan Journal of Law Reform

Volume 42

2009

Privacy 3.0-The Principle of Proportionality

Andrew B. Serwin
Foley & Lardner LLP

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.

---

* Andrew Serwin is the founding chair of the Privacy Security and Information Management Practice and a partner at 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 *Information Security and Privacy: A Practical Guide to Federal, State and International Law*, a 3,600 page treatise on information security and privacy, which has been called "the best privacy sourcebook," "an indispensible resource for privacy professionals at all levels," and "a book that everybody in the information privacy field should have on their desk," and the *Internet Marketing Law Handbook*, both published by Thomson-West. He has written over seventy articles, predominantly on information management and Internet issues, is also the author of the advertising section of the 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 *Selling Products and Services and Licensing Software Online: An Interactive Guide With Legal Forms and Commentary to Privacy, Security and Consumer Law Issues.* Mr. Serwin was ranked by Chambers USA – 2009 in the area of National: Privacy & Data Security, where he was described by clients as "a tireless worker, holding onto the ever-shifting puzzle pieces of the law in this area in a way that other privacy lawyers cannot".

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.

The author would like to acknowledge Chris Hoofnagle, James Kalyvas, Kristopher Keys, Peter McLaughlin, Michael Overly, and William Yoon for their valuable suggestions to this Article.

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.

INTRODUCTION

Individual concern over privacy has existed for 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 eaves of their houses. This concern changed as technology evolved in the late 1800s, 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,

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's and Brandeis's article, see Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007).

while serving on the Supreme Court, 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 changed, a belief surfaced that the Warren and Brandeis formulation did not provide sufficient structure for the development of privacy laws.[5] As such, a second theoretical construct of privacy, Privacy 2.0, as expressed in Dean Prosser's work *Privacy*, was created and ultimately captured in the *Restatement (Second) of 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 four distinct acts that were found to be violations of an individual's right of privacy. While important, Prosser's theory is limited because its basis, like that of Privacy 1.0, stems from common law and tort.

These works, while influential in their time, do not account for changes in values, paradigm shifts in technology, and, 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 privacy issue that looms on the horizon, health care record interoperability, provides a perfect example of changes in technology effecting societal norms regarding privacy. Many states are mandating health care entities that receive state funds to become

3. Olmstead v. United States, 277 U.S. 438 (1928).

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

5. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

compliant with systems that permit the sharing of medical information electronically by 2014.[6] While setting the technological standards is a difficult task, setting the standards for privacy and security will present even more complex challenges. In the time of Warren and Brandeis, a "right to be let alone" was a viable theoretical construct.[7] In today's society, information sharing is 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.[8]

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.[9] Despite the proliferation of privacy laws in the United States, more and more people feel they have less protection for their personal information.[10] That the

---

6. On February 17, 2009, President Barack Obama signed into law the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (2009) ("ARRA") (commonly referred to as the Federal Stimulus Package). The ARRA contained the Health Information Technology for Economic and Clinical Health Act's ("HITECH Act") provisions within it. The ARRA provides for substantial stimulus expenditures in the health care industry, particular for the adoption of electronic health records ("EHR") technology. The largest allocation of healthcare information technology ("HIT") related funding—approximately $16 billion—is for incentives through the Medicare and Medicaid reimbursement systems to incentivize providers and hospitals to implement EHR systems.

7. Warren & Brandeis, *supra* note 4, at 205.

8. 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 when 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.

9. *See, e.g.*, Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643 (2007); Richards & Solove, *supra* note 2.

10. Indeed, Dean Chemerinsky recently noted that informational privacy:

> [I]s 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 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 9, at 656–57.

European Union (EU) found 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.[11]

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.[12] 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."[13] 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.[14]

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. Indeed, when they are assessing constitutional rights of individuals regarding the disclosure of information, many courts are starting to recognize and reject the concept of "confidentiality" and examine whether information is "sensitive," thus not considering whether the information is "public" or "private."[15]

---

11. 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 principles, or enacting Binding Corporate Rules. For a complete discussion of these concepts, see ANDREW SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE, AND INTERNATIONAL LAW (2nd ed. West 2008).

12. Chemerinsky, *supra* note 9, at 644.

13. Richards & Solove, *supra* note 2, at 127–30.

14. Richards & Solove, *supra* note 2, at 131–32.

15. *See* Doe v. Poritz, 662 A.2d 367, 410 (N.J. 1995) ("[P]rivacy interests may be implicated where disclosure of a person's address results in unsolicited contact .... We find, moreover, that considering the totality of the information disclosed to the public, the Notification Law implicates a privacy interest. That the information disseminated under the Notification Law may be available to the public, in some form or other, does not mean that plaintiff has no interest in limiting its dissemination."); Burnett v. County Of Bergen, 954 A.2d 483 (N.J. Super. Ct. App. Div. 2008) (holding that disclosure of Social Security numbers violated the New Jersey state constitution even though Social Security numbers are frequently public), *aff'd in part and rev'd in part*, 968 A.2d 1151 (N.J. 2009).

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, but it cannot account for the technology and societal values of today, our statutorily-driven privacy protections, and the Federal Trade Commission (FTC) enforcement centric model, and should therefore not provide the theoretical construct for existing or future laws or court decisions. *This is all the more true in light of recent FTC guidance regarding behavioral advertising, in which the FTC expressly recognized the need to balance support for innovation and consumer protection, as well as the "benefits" provided to consumers by behavioral advertising.*[16]

The experience of the last one hundred 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.[17] 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

16. *See* FEDERAL TRADE COMMISSION, ONLINE BEHAVIORAL ADVERTISING MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (2007) (on file with the University of Michigan Journal of Law Reform), *available at* www.ftc.gov/os/2007/12/P859900stmt.pdf.

17. Warren and Brandeis explicitly state that tort enforcement is the appropriate mechanism to enforce privacy Warren & Brandeis, *supra* note 4, at 219, as does Prosser, which is demonstrated by the adoption of his four categories of privacy violations into the *Restatement (Second) of Torts*, RESTATEMENT (SECOND) OF TORTS §§ 652A–E (1976).

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.[18] All a common law based model will ensure is that, in many cases, these laws will impose inconsistent burdens on information that will not meet society's need for privacy.[19]

Given the changes in society, as well as the enforcement mechanisms that exist today, particularly given the FTC's new focus on "unfairness," and the well-recognized need to balance regulation and innovation, a different theoretical construct must be created—one that 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 in fact they have much to lose) from overbroad privacy restrictions.[20] For instance, overbroad privacy restrictions could jeopardize someone's life if the sharing of medical information is hindered in an emergency

18. 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, 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, *supra* note 11, at chs. 5–6, 14 (discussing the law of pretexting and wiretapping).

19. For a detailed treatment of privacy law, see SERWIN, *supra* note 11.

20. As noted below, this concept is implicit in the FTC's formulation of what is an "unfair" business practice, which is a now a privacy and security enforcement theory. *See infra* Part V.

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 the 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. The four tiers will provide guidance on existing issues, attempt to bring cohesion to the numerous state and federal laws, and 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 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.

The proportionality framework could also address more easily the changes in societal norms and values. As we have seen from the meteoric rise of the Internet and related technologies, new technology both generates new privacy concerns (through the creation of new forms of sensitive data) and renders certain privacy concerns related to older technology (that is no longer used) less relevant. Once data becomes less important or relevant (think of the relative unimportance of the PIN for your ATM if banks started using biometric data as an authenticator), the information becomes less sensitive. The principle of proportionality, with its focus

on the level of sensitivity of information, can accommodate those changes in a way that other models cannot.

The need for a meaningful and relevant theoretical construct for privacy cannot be overstated. Statutes and case law ultimately set the standards for conduct and provide guidance after they are enacted or decided. However, setting up a theoretical construct a priori such that it could be used proactively by legislators and courts when confronting privacy issues will help minimize inconsistent requirements that either are too restrictive (therefore creating economic and other barriers for society) or not restrictive enough to protect privacy.

One issue should be noted before the matrixed model is examined. While in theory the model could be based upon a continuum, the use of a matrixed approach would cause the model to lose some of its predictive ability. The loss of predictive ability would result from the inability to group similar types of information into tiers and it is this grouping that lets individuals more accurately predict how new forms of information will be treated.

I. PRIVACY 1.0—A HISTORICAL BACKGROUND

While privacy was not invented by Warren and Brandeis, *The Right to Privacy* was, and remains, 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.[21]

Warren and Brandeis were deeply concerned about the inability of the common law to protect an individual's privacy, particularly at a time of technological advances:

> 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.[22]

21. Prosser, *supra* note 5, at 423.
22. Warren & Brandeis, *supra* note 4, at 196.

The technological advance that caused the most concern was the instant camera.[23]

> 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 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.[24]

While the problem was clearly identified by Warren and Brandeis, finding a legal theory that provided adequate protection proved more difficult.[25] 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.[26]

However, the law of defamation was ultimately rejected because it was based upon a "radically different class" of damages to an individual.[27] This was in part because, if the action was otherwise lawful,

---

23. 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 forty-year period between 1850 and 1890 the number of newspapers grew from one-hundred to nine-hundred, with a corresponding increase in readers. Newspaper readers went from approximately 800,000 to more than 8 million people. Richards & Solove, *supra* note 2, at 128.

24. Warren & Brandeis, *supra* note 4, at 195–96.

25. "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 197.

26. Warren & Brandeis, *supra* note 4, at 197.

27. "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 . . . . [T]he wrongs and

common law, unlike Roman law, did not recognize a claim for mere mental injury.[28]

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 trust or confidence.[29]

Despite this observation, they ultimately rejected this theory, finding that a contractual theory was too narrow to address the privacy harms of the day.[30]

Warren and Brandeis then concluded that the extension of common law could address privacy concerns. They noted that "[t]he common law secures to each individual the right of

---

correlative rights recognized by the law of slander and libel are in their nature material rather than spiritual." Warren & Brandeis, *supra* note 4, at 197.

28. Warren & Brandeis note that:

> 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 197–98.

29. Warren & Brandeis, *supra* note 4, at 207.

30. Warren & Brandeis note that:

> This process of implying a term in a contract, or of implying a trust (particularly where a contract is written, and where these 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 210–11.

determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[31] This right was seen as a broad right of privacy against an individual, irrespective of privity of contract.[32] 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."[33] While Brandeis receives credit for inventing this right, as noted above, in fact Judge Thomas Cooley coined the phrase in a tort treatise.[34] Warren and Brandeis explicitly relied upon common law theories, as well as common law enforcement. They saw actions for tort damages as a critical part of the enforcement of the right of privacy.[35]

Richards and Solove question the use of the right to be let alone as a privacy concept. Judge Cooley originally used the concept in the context of a plaintiff who had suffered an assault where no physical contact occurred.[36] In modern parlance, this would be an intentional 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.[37]

---

31. Warren & Brandeis, *supra* note 4, at 198.
32. Warren & Brandeis note that:

> 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 213.

33. Warren & Brandeis, *supra* note 4, at 205.
34. Richards & Solove, *supra* note 2, at 129–30.
35. Warren & Brandeis note that:

> [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.

Warren & Brandeis, *supra* note 4, at 211.

36. Richards & Solove, *supra* note 2, at 130.
37. Richards & Solove note that:

The right to be let alone, despite being rooted in the law of assault, and not privacy, became one of the enduring privacy concepts.[38] Not only did it appear in *The Right to Privacy*, it also appeared in one of Justice Brandeis's 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.[39]
>
> 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.[40]

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.[41]

> 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.
>
> Richards & Solove, *supra* note 2, at 130.

38. Warren & Brandeis, *supra* note 4, at 205.
39. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
40. *Id.* at 473.
41. Richards & Solove note that:

> 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.

While Warren and Brandeis's article was hailed and treated as the theoretical construct for privacy for over one hundred years, recently modern scholars have begun to question its continuing viability. Richards and Solove, relying upon English common law, argue that Warren and Brandeis should have followed a different path—one that rests on claims arising out of a "breach of confidence," instead of relying, as noted above, on one that protects an "inviolate personality" from harm.[42]

Moreover, ironically, given that the technological driver of Warren's 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.[43] While not directly questioning the Warren and Brandeis model, it is notable that the very issue that Warren and Brandeis wrote about still defies current privacy theory.

II. 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. Dean Prosser noted this disconnect in 1960:

---

42. Richards & Solove note that:

> 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.

Richards & Solove, *supra* note 2, at 133.

43. On this point, the law review noted that:

> 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.

Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1872 (2007).

> 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 forms of invasions, and to realize that they call for different things.[44]

Dean Prosser attempted to cure the disarray by creating the next theoretical construct of privacy—Privacy 2.0—by 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's four categories of privacy torts: intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a 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 invades, physically or otherwise, the solitude or seclusion of another or his private affairs or concerns, if the intrusion would be highly offensive to a reasonable person.[45] 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.[46] This theory tracks the Privacy 1.0 model quite closely.

Appropriation of name or likeness occurs when a person makes use of the name or likeness of another.[47] 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, where 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.[48] Both of these theories also track closely the Privacy 1.0 analysis, though they are more focused on the imposition of liability. Finally, the Restatement imposes liability for publicity placing a person in false light.[49] This theory would seem to be

---

44. Prosser, *supra* note 5, at 407.
45. RESTATEMENT (SECOND) OF TORTS § 652B (1976).
46. *Id.* § 652B cmt. a.
47. *Id.* § 652C.
48. *Id.* § 652D.
49. *Id.* § 652E.

encompassed in prior theory, but Prosser believed that Warren and Brandeis did not deal with this directly.[50]

III. THE WEAKNESSES OF COMMON LAW THEORIES

While the Prosser/Restatement model provides some additional framework to understand privacy concepts, it still relies on common law, and is still based in tort theory. Inherently, this limits its usefulness in addressing the privacy issues of today. One of the limitations of a common law/tort based model is at some level foreshadowed in the Warren and Brandeis article. Specifically, when Warren and Brandeis dismissed property law as a basis for the enforcement of privacy rights, they noted that "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 as one of property."[51] 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 certainly demonstrates the difficulty that tort-based theories face in addressing the privacy issues of a Web 2.0 world. Indeed, today numerous courts find that tort liability does not exist in privacy cases that arise from the misuse of electronic information where there is no economic loss. Thus, these courts seem to decide, just as 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.[52]

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 alterative 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. However, in many of today's privacy laws (such as the Health Insurance Portability and Accountability Act

50. "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.

51. Warren & Brandeis, *supra* note 4, at 200.

52. *Id.*

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 protections of our time, including "mitigation" statues, as well as credit freeze laws and identity theft laws that restrict the misuse of information of deceased individuals.[53]

IV. 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 *Trikas*,[54] one of the first of such cases, the court rejected a plaintiff's claim for violation of the Fair Credit Reporting Act. In this case, 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.[55] Under the theory espoused by Warren and Brandeis, along with modern scholars, liability should have attached. However, the court dismissed the claim because the plaintiff could not prove that the alleged violation caused any damages 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 did not comply with its privacy 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

53. 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.

54. Trikas v. Universal Card Serv. Corp., 351 F. Supp. 2d 27 (E.D.N.Y. 2005).

55. *Id.* 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 SERWIN, *supra* note 11, at ch. 26.

Dyer v. Northwest Airlines Corps.,[56] 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's posted privacy policy.[57] Northwest advanced two theories to defeat the plaintiffs' claims. First, that its online policy was not a contract, but rather an aspirational policy whose violation 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.[58]

In *Stollenwerk v. Tri-West Healthcare Alliance*,[59] 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. Some of the plaintiffs did not suffer identity theft, but they 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.[60]

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.[61] 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[62] by deciding that even though one of the plaintiffs had

56. 334 F. Supp. 2d 1196 (D.N.D. 2004).

57. *Id.* at 1197.

58. *Id.* at 1199–1200; *see also In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552 (N.D. Tex. 2005).

59. No. Civ. 03–0185PHXSRB, 2005 WL 2465906, at *1 (D. Ariz. Sept. 6, 2005).

60. *Id.*

61. *Id.* at *4.

62. *Id.* ("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.").

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.[63]

The Ninth Circuit reviewed this decision and modified the analysis.[64] While it still upheld the dismissal of two of the three plaintiffs' claims and completely rejected the medical monitoring analogy, it reversed the judgment in favor of the third plaintiff, finding that, given the unique factual circumstances, there could be potential damages that flowed from the alleged disclosure of information. It therefore reversed in part, affirmed in part, and remanded the case.[65] The district court in *Forbes v. Wells Fargo Bank* reached a similar conclusion.[66] In this case, the plaintiffs' personal information was obtained through a theft of computers that contained unencrypted customer information including names, addresses, social security numbers and account numbers. Again, it 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. Consistent with the other decisions cited above, the court rejected the plaintiffs' claim that they had suffered damage as a result of the time and money they had spent to monitor their credit, because the plaintiffs could not prove a loss of earning capacity or wages.[67] The court therefore rejected both the breach of contract and negligence claims.

In *Bell v. Acxiom*, the court addressed the issue of damages in a privacy case arising out of a computer hacking incident.[68] The plaintiff alleged that the hacking incident compromised her personally identifiable information and that "lax security" left her at risk for privacy issues and for receiving junk mail.[69] The main issue addressed was whether the plaintiff had standing to pursue the claim. Standing typically requires that a plaintiff satisfy three requirements: (1) that the plaintiff has suffered injury which is actual, concrete, and particularized; (2) that there is a causal connection between the conduct complained of and the injury; and (3) that the injury will be redressed by a favorable decision.[70] It

63. *Id.* at *7.

64. *See* Stollenwerk v. Tri-West Health Care Alliance, 254 Fed. Appx. 664, 668 (9th Cir. 2007).

65. *Id.* at 669.

66. 420 F. Supp. 2d 1018 (D. Minn. 2006).

67. *Id.* at 1020–21.

68. No. 4:06CV00485-WRW, 2006 WL 2850042, at *1 (E.D. Ark. Oct. 3, 2006).

69. *Id.*

70. *See id.*; *see also* Lujan v. Nat'l Wildlife Fed'n, 497 U.S. 871, 889 (1990) (citing United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S. 669 (1973)); Whitmore v. Arkansas, 495 U.S. 149 (1990); City of L.A. v. Lyons, 461 U.S. 95

should also be noted that the plaintiff has the burden of proof on these issues[71] and that potential, future injuries do not constitute a sufficient showing by the plaintiff.[72] In this case, because the plaintiff could not show injury or even that she received any junk mail, the court dismissed her case.[73]

Similar conclusions have been reached by other courts, including in *Key v. DSW, Inc.*[74] Recently, in *Kahle v. Litton Loan Servicing, LP*, an Ohio court followed the DSW decision by finding that economic harm was a prerequisite for a plaintiff to state a claim for damages.[75] *Kahle* concerned a security breach that could have resulted in the disclosure of the plaintiff's personal information.[76] The defendant advised all affected individuals to place a credit freeze on their report.[77] The plaintiff could not establish any direct damages, other than costs associated with a credit monitoring service that the plaintiff purchased.[78] The court dismissed the claim, holding that any alleged damages were too speculative, particularly since the defendant had advised the plaintiff to place a free fraud alert on her credit report.[79] The court dismissed the claim despite the fact that the plaintiff was seeking reimbursement of monies paid for a credit monitoring service.[80] In 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.[81] The lack of damages issue has also been addressed in the

---

(1983); Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26 (1976); O'Shea v. Littleton, 414 U.S. 488 (1974).

71. *See Bell*, 2006 WL 2850042, at *1–2 (citing Shain v. Veneman, 376 F.3d 815, 817 (8th Cir. 2004), *cert. denied*, 543 U.S. 1090 (2005); Delorme v. United States, 354 F.3d 810, 815 (8th Cir. 2004)).

72. *Id.* at *2 (citing Sierra Club v. Robertson, 28 F.3d 753, 758 (8th Cir. 1994); Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

73. Even if plaintiff had shown that she received junk mail, it is unlikely whether this would have been a sufficient showing of injury. *Id.* at *2 (citing Walters v. DHL Express, No. 05-1255, 2006 WL 1314132, at *5 (C.D. Ill. May 12, 2006)).

74. 454 F. Supp. 2d 684, 688–89 (S.D. Ohio 2006) (citing Inge v. Rock Fin. Corp., 281 F.3d 613, 619 (6th Cir. 2002)) ("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.").

75. 486 F. Supp. 2d 705, 709–10 (S.D. Ohio 2007).

76. *Id.* at 706.

77. *Id.* at 707.

78. *Id.* at 709–713.

79. *Id.* at 712–13.

80. *Id.* at 713.

81. *See, e.g.*, Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1 (D.D.C. 2007) (dismissing claim for future identity theft arising from the theft of a laptop computer).

context of the Fair Credit Reporting Act (FCRA),[82] at least for claims of actual damages.[83] FCRA does, however, permit recovery of statutory damages for willful violations and claims without damages can, sometimes, survive.[84] This was also the conclusion in cases involving American Airlines[85] and JetBlue.[86]

The failings of tort theory also are apparent when one considers how the law typically treats cyber defamation cases. The Communications Decency Act[87] provides broad immunity to publishers on the Internet for postings by third-parties and this law reflects the decision of Congress to protect the Internet from "overzealous" laws. 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.[88] 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 on tort law concepts has significant limitations, at least at this point in jurisprudence. This is especially true since government enforcement is frequently the motivating factor for privacy compliance.

V. 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.[89] The FTC is the main privacy enforcement agency at the federal level and truly sets the tone for privacy

82. 15 U.S.C. § 1681 (2006).

83. Schroeder v. Capitol Indemnity Corp., No. 05-C-643, 2006 WL 2009053, at *1 (E.D. Wis. July 17, 2006) (granting summary judgment, in part, and dismissing portion of claim under FCRA because plaintiff failed to provide evidence of actual injury).

84. *Id.* at *4–5 (citing Murray v. GMAC Mortgage Corp., 434 F.3d 948 (7th Cir. 2006)).

85. *In re* American Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 567 (N.D. Tex. 2005).

86. *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (holding loss of privacy is not a recoverable damage under a breach of contract theory).

87. 47 U.S.C. § 230 (2006).

88. *See* Zeran v. American Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997); *see also* SERWIN, *supra* note 11, § 2:6–2:16.

89. *See generally* FEDERAL TRADE COMMISSION, *supra* note 16.

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 (the FTC Act), one of the main bases of the FTC's enforcement power, makes "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce" unlawful.[90] While the deceptiveness prong of Section 45 was the more common enforcement mechanism, as discussed below, recent cases have increasingly relied on the unfairness prong of the FTC Act.[91]

The most recent guidance from the FTC, *Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles*, seems to match the ideas behind the principle of proportionality.[92] In this publication the FTC recognizes the need to balance support for innovation with the need to protect consumers from harm.[93] Moreover, the FTC also acknowledged the benefits that consumers derive from information sharing, including free information and services on the Internet.[94] Finally, the FTC noted that, for purposes of data security, the sensitivity of the data is an important factor in coming up with a behavioral advertising framework.[95] This was the case because, while certain forms of data collected for behavioral advertising are sensitive, there are other forms that are not identifiable and therefore not as problematic if wrongfully acquired. Both concepts are difficult for tort law to address, but they are inherently consistent with the principle of proportionality.

In re Vision I Properties, LLC concerned an FTC investigation of a company that licensed shopping cart software and related services to online retailers.[96] These websites made specific representations regarding privacy, including that personal information was not sent, sold, or leased to third-parties.[97] The FTC alleged that Vision I violated the FTC Act[98] because the portions of the websites that

90. 15 U.S.C.A. § 45(a)(1) (West 2009).

91. See, for example, *In re* BJ's Wholesale Club, Inc., File No. 042-3160, 2005 WL 1541551 (F.T.C. June 16, 2005), 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.

92. *See generally* FEDERAL TRADE COMMISSION, *supra* note 16.

93. *See id.* at 1.

94. *See id.* at 2.

95. *See id.* at 4.

96. Docket No. C-4135, File No. 0423068, 2005 WL 1274741 (F.T.C. Apr. 19, 2005).

97. *Id.*

98. This matter involved a draft complaint that was not filed because the matter was resolved via consent order.

gathered customers' information were Vision I's which did not disclose to customers that the privacy practices on these pages were different from other pages, despite the fact that the pages appeared to be part of the same website.[99] The FTC claimed that Vision I also rented the customers' information to third-parties, despite the privacy statements made by the retailers.[100] Furthermore, Vision I allegedly failed to disclose to its clients Vision I's practice of renting out customer information.[101] The FTC considered these acts to be violations of the FTC Act.[102] The consent order that was entered into by Vision I restricted its ability to disclose customers' personally identifiable information, required it to pay certain costs, mandated additional disclosures regarding Vision I's privacy practices and placed it under reporting obligations to the FTC.[103]

The importance of this enforcement action was that, unlike prior enforcement cases, there was no direct representation to consumers by Vision I—a standard prerequisite for deceptive practices under Section 45. Thus, 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 the "unfairness" prong of the FTC Act in *In re BJ's Wholesale Club, Inc.*[104] This case represents a marked departure from prior FTC actions in that the FTC relied upon its unfairness authority and, unlike prior enforcement cases, did not rely upon an allegedly deceptive statement regarding information security. BJ's Wholesale Club operates a number of membership warehouse stores.[105] As part of its normal business, BJ's accepted credit cards as a form of payment from its members.[106] BJ's collected personally identifiable information from its customers to authorize their credit cards.[107] It also used wireless technology, including wireless access points and scanners to monitor inventory.[108] The FTC filed a complaint against BJ's, alleging that BJ's 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

99. *Vision I Properties*, 2005 WL 1274741.
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. File No. 042-3160, 2005 WL 1541551 (F.T.C. June 16, 2005).
105. *Id.*
106. *Id.*
107. *Id.*
108. *Id.*

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.[109]

The FTC alleged that, as a result of this conduct, millions of dollars in fraudulent purchases had been made.[110] Although BJ's conduct did not directly violate any federal statute, the FTC concluded that these acts constituted an unfair business practice under the FTC Act and brought an enforcement action against BJ's.[111] 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,[112] the Children's Online Privacy Protection Act,[113] and the Gramm-Leach Bliley Act[114]) or when 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.[115]

The use of the unfairness doctrine by the FTC is consistent with the principle of proportionality because the unfairness doctrine examines the unreasonable harm to consumers which, at least in part, rests upon the sensitivity of data. While the unfairness doctrine is an evolving one, the FTC did provide some guidance regarding what constitutes an unfair practice when it issued its Unfairness Statement[116] in 1980. The Commission stated that "[u]njustified consumer injury is the primary focus of the FTC

109. *Id.*

110. *Id.*

111. *Id.*

112. Health Insurance Portability and Accountability Act, 110 Stat. 1936 (1996).

113. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (West 2009).

114. Gramm-Leach-Bliley Fin. Serv. Modernization Act, 113 Stat. 1338 (1999).

115. While *In re BJ's Wholesale Club, Inc.* 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 re ReverseAuction.com, Inc.* matter. Mozelle Thompson, Statement of Comm'r Mozelle W. Thompson in *In re* ReverseAuction.com, Inc., File no. 0023046 (2000) (on file with the University of Michigan Journal of Law Reform), *available at* http://www.ftc.gov/os/2000/01/reversemt.htm. 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. *Id.*

116. Letter from the Federal Trade Commission to Hon. Wendell Ford and Hon. John Danforth, Comm. on Commerce, Science and Transp. (Dec. 17, 1980), *reprinted in In re Int'l Harvester Co.*, 104 F.T.C. 1070 (1984).

Act"[117] 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."[118] The FTC added 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."[119]

The formulation of the FTC's Unfairness Statement is important, particularly now that the FTC is using unfairness as a basis for enforcement actions. Thus, 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.

The failing of theories based upon confidentiality has been recognized by some courts. In *Burnett*, a New Jersey Court addressed whether the constitutional right of privacy expressed in a state constitution protected the disclosure of Social Security numbers in records that were otherwise public records.[120] The fact that Social Security numbers were not always non-public did not stop the court from concluding that the disclosure of Social Security numbers violated the New Jersey constitution.[121] This conclusion has been reached by other courts that have found the disclosure of Social Security numbers can violate individuals' rights of privacy, including under the federal and state constitutions, as well as public records laws.[122] Part of the issue with Social Security numbers is the potential for misuse that courts have noted:

> While the release of all city employees' [social security number]s would provide inquirers with little useful information about the organization of their government, the release of the numbers could allow an inquirer to discover the intimate,

---

117. *In re Int'l Harvester Co.*, 104 F.T.C. at 1073; *see also* SERWIN, *supra* note 11, § 12:1–12:7.

118. *In re Int'l Harvester Co.*, 104 F.T.C. at 1073–74.

119. *Id.* at 1075.

120. Burnett v. County Of Bergen, 954 A.2d 483, 484 (N.J. Super. Ct. App. Div. 2008).

121. *Id.* at 497.

122. *See, e.g.*, Aronson v. Internal Revenue Serv., 767 F. Supp. 378, 388 (D. Mass. 1991); Oliva v. U.S., 756 F. Supp. 105, 107 (E.D.N.Y. 1991); Data Tree, LLC v. Meek, 109 P.3d 1226, 1237–38 (Kan. 2005); Zink v. Commonwealth, 902 S.W.2d 825, 829 (Ky. Ct. App. 1994); State *ex rel.* Beacon Journal Publ'g Co. v. City of Akron, 640 N.E.2d 164, 165–66 (Ohio 1994), *reconsideration denied*, 642 N.E.2d 388 (Ohio 1994); Tribune-Review v. Allegheny County Hous. Auth., 662 A.2d 677, 683 (Pa. Commw. Ct. 1995).

> personal details of each city employee's life, which are completely irrelevant to the operations of government. As the *Greidinger* court warned, a person's SSN is a device which can quickly be used by the unscrupulous to acquire a tremendous amount of information about a person.[123]

Thus, sensitivity, not confidentiality, was the touchstone of the court's analysis. Certain courts have held that, though sensitive information is publicly available, there still may be a protectable right that precludes disclosure. In addressing the disclosure of addresses, one court noted:

> It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but "[in] an organized society, there are few facts that are not at one time or another divulged to another." The privacy interest protected by Exemption 6 "encompass[es]the individual's control of information concerning his or her person." *An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.*[124]

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 that these privacy principles are not needed. 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. The need for principles to guide privacy law can be seen by the number of countries that have adopted principle-based statutes. It is also shown by organizations such as the Organisation for Economic Co-operation and Development (OECD), which was one of the first organizations to promulgate privacy principles through non-binding guidelines. Though the United States is a member of the OECD, it has not adopted these concepts in any way. However, these principles form the theoretical framework for the European Union's Data Directive, which created the privacy protections that

123. *Beacon Journal*, 640 N.E.2d at 169 (citing Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993)).

124. Doe v. Poritz, 662 A.2d 367, 409 (1995) (emphasis added).

exist in the EU today. The first principle of the OECD Guidelines is collection limitation which calls for "limits to the collection of personal data" along with requirements that "any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[125] The second principle concerns data quality and it requires that personal data "be relevant to the purposes for which they are used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."[126] The third principle is purpose specification which mandates that the reason for personal data collection be specified at the time of data collection and that the subsequent use be limited to the fulfillment of these purposes or other compatible purposes that must be specified on each occasion of change of purpose.[127] 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 [these requirements] except with the consent of the data subject; or by the authority of law."[128]

The fourth OECD principle covers security safeguards. "Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data."[129] The fifth principle is openness and the Guidelines suggest that "[t]here should be a general policy of openness about developments, practices and policies with respect to personal data."[130] Additionally, readily available means should exist to establish "the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[131] The sixth principle relates to individual participation.[132] The Guidelines suggest certain

125. ORG. FOR ECON. COOPERATION & DEV., RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROT. OF PRIVACY AND TRANSBORDER FLOWS OF PERS. DATA § 7 (1980) [hereinafter OECD, RECOMMENDATION].

126. *Id.* § 8.

127. *Id.* § 9.

128. *Id.* § 10.

129. *Id.* § 11.

130. *Id.* § 12.

131. *Id.* § 12. "'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." ORG. FOR ECON. COOPERATION & DEV., OECD GUIDELINES ON THE PROT. OF PRIVACY AND TRANSBORDER FLOWS OF PERS. DATA § 1(a) (1980) [hereinafter OECD, GUIDELINES].

132. OECD, RECOMMENDATION, supra note 125, § 13.

controls and limitations that place restrictions that are reasonably related to the use and collection of the data.[133]

The seventh principle pertains to accountability and it suggests that a data controller should be responsible for complying with measures that give effect to these principles.[134] The eighth and final principle covers international application. The Guidelines encourage member countries to consider "the implications for other [m]ember countries of domestic processing and re-export of personal data."[135] Member states are also encouraged to "take all reasonable and appropriate steps to ensure that transborder flows of personal data,[136] including transit through a member country," remain "uninterrupted and secure."[137] A member country is cautioned to "refrain from restricting transborder flows of personal data between itself and another [m]ember country except where the latter does not substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation."[138]

The Asia-Pacific Economic Cooperation (APEC) also adopted principles that have served as the basis for privacy legislation in the Pacific Rim.[139] APEC's guidelines, which are similar to OPEC's, consist of preventing harm, providing notice, limiting data collection, regulating uses of personal information, choice (regarding collection and use), ensuring integrity of personal information, developing security safeguards, controlling access and correction (to rectify any inaccuracies), and establishing accountability.[140]

These concepts are important to note because they demonstrate that principles can dramatically impact privacy legislation, since these serve as the theoretical construct of the EU Data Directive.[141] As discussed below, even England implemented the OECD principles instead of its own common law in constructing a theoretical framework for privacy laws.

---

133. OECD, RECOMMENDATION, supra note 125, § 13(a)–(d).

134. *Id.* § 14.

135. *Id.* § 15.

136. "'Transborder flows of personal data' means movements of personal data across national borders." OECD, GUIDELINES, *supra* note 131, § 1(c).

137. OECD, RECOMMENDATION, supra note 125, § 16.

138. *Id.* § 17.

139. See SERWIN, *supra* note 11, at ch. 1 for a complete discussion of these principles.

140. SERWIN, *supra* note 11, § 1:16.

141. *Id.*

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 damages 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.[142] Perhaps more importantly, it did so through the adoption of a number of principles that in no way relate to the common law theory of confidences. Although English law does not explicitly recognize proportionality, its distinctions between personal data[143] and sensitive personal information[144] resemble the tiers created by the application of the principle of proportionality.

The United Kingdom's Data Protection Act of 1998 mandates compliance with eight key principles for anyone processing personal information. These key principles require "that personal

142. *Id.*

143. "'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, c. 29, pt. I, § 1 (Eng.).

144. 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.

Id. at c. 29, pt. I, § 2.

information is: fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate and up to date; not kept longer than is necessary; processed in line with [individuals'] rights; secure; not transferred to other countries without adequate protection."[145] Nowhere in these principles is the concept of confidence. Thus, if we are to look for a framework to follow for United States law, it should not be one 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, because the United States has shown no real interest in adopting a principle-based law, though they do impact United States companies in certain circumstances.

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, U.S. law does not exclude these 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.[146] This resulted in the creation of the safe harbor program which allows American companies conducting trans-Atlantic transactions to comply with the EU privacy requirements in a simplified manner.[147] A United States company could certify that it complied with the safe harbor principles and then transfer data from the EU to the United States.[148] There are seven U.S. privacy principles and they are: notice, choice, onward transfer, access, security, data integrity, and enforcement.[149]

---

145. Information Commissioner's Office, The Data Prot. Act: The Basics, http://www.ico.gov.uk/what_we_cover/data_protection/the_basics.aspx. (last visited May 14, 2009) (on file with the University of Michigan Journal of Law Reform).

146. Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited June 13, 2009) (on file with the University of Michigan Journal of Law Reform).

147. *Id.*

148. *Id.*

149. U.S. DEPT. OF COMMERCE, SAFE HARBOR PRINCIPLES (2000) (on file with the University of Michigan Journal of Law Reform), *available at* http://www.export.gov/safeharbor/eu/sh_en_privacy1.asp.

While they exist, these principles do not serve as the theoretical construct for privacy laws in the United States. Although the Internet and electronic communications are world-wide technologies, it is notable that the United States has not adopted the concepts 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

Concerns over privacy in the United States relate less to concepts such as publicity given to private life, because at least in certain circumstances many people actually seek out opportunities to publicize private aspects of their lives. Social networking, blogging, and relatively easily obtainable consumer credit all depend on information sharing to function. 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 rooted in the U.S., but the liberal American view of information sharing may be the reason why social networking web sites originated in the U.S.

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. 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 publication 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, particularly at a time of increased reliance on computers for information. In one of the more colorful discussions of the issue, one Ninth Circuit judge 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.[150]

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.

XI. PRIVACY 3.0

Given the current rapid progress of technology, 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 recent pretexting debate and its resulting flurry of laws. Moreover, the theory should provide a unifying principle to understand both the numerous current privacy laws and those being enacted at an increasing pace, 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 focusing 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 more relevant 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

150. United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir. 2006) (en banc) (Kleinfeld, J. dissenting).

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 types 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[151] (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, must also be considered when placing a category of information into a tier. The social utility of sharing of information will also be considered, as well as 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.[152] Whether the information can be used to obtain or create other information (such as a Social Security number) is a further factor that affects 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 used by courts in Fourth Amendment cases, as well as trade secret cases involving proprietary information, the steps the person or business took to protect the privacy of the information represent a critical factor as well.[153]

Once information is placed into a tier, predicting how it can be collected and used is possible, because information collection, management, processing, use, and disposal all flows from the tier within which the category of information falls. Thus, there are common elements that I will be discussing regarding each tier. These include:

---

151. 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.

152. 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.

153. *See* Rakas v. Illinois, 439 U.S. 128, 152–53 (1978) ("The ultimate question, therefore, is whether one's claim to privacy from government intrusion is reasonable in light of all the surrounding circumstances.").

- 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.

While in the vast majority of cases the state and federal government have followed a similar path and the protection afforded by the law is consistent, others have 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.[154]

A. Tier I—Highly Sensitive Information

Tier I information would cover extremely sensitive[155] information and would be subject to strong limitations on collection, processing and disclosure, though in certain extremely limited instances, the information could be collected and used without

154. 18 U.S.C.A. § 1030 (West 2009).

155. 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. *See, e.g.*, United States 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.

consent, particularly by the government. Examples of Tier I data would include genetic information, sexual history or other related issues, religious affiliation, information regarding communicable diseases, various 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, and images or videotapes of conduct in private areas. Radio Frequency Identification (RFID) may ultimately fall within this category and, despite the current debate, so will Passenger Name Records (PNR) and other forms of location tracking.[156]

Generally these types of information cannot be gathered without the express consent of the data subject, unless there is a truly compelling governmental purpose, such as national security or crime prevention, and even then, only in limited circumstances. For example, government agencies can collect DNA of offenders convicted of certain crimes and this information can be processed for a limited period of time in a computer software program known as CODIS for the purpose of solving crimes.[157] 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.[158]

However, if the data subject gives consent, processing and use of such information would be permitted, but only in limited circumstances. Moreover, there frequently are time restrictions on the retention of the information as well as requirements of high levels of data security. Violation of laws pertaining to Tier I information should give rise to severe civil and even criminal sanctions.

---

156. The acquisition of location tracking 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. *In re* Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register and Caller Identification Sys. on Tel. Nos. and the Prod. of Real Time Cell Site Info., 415 F. Supp. 2d 663 (S.D. W. Va. 2006); *but c.f. In re* Application of U.S. for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a PIN Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (permitting the gathering of location tracking information); *In re* Application for Pen Register and Trap/Trace device with Cell Site Location Auth., 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. *See* SERWIN, *supra* note 11, § 5:67.

157. *See* SERWIN, *supra* note 11, §§ 31:51–52.

158. *See id.* § 11:48

B. Tier II—Sensitive Information

Tier II would cover still quite sensitive information which would not rise to the same level of sensitivity as Tier I information. Examples of Tier II information would include the content of wire or electronic communications (if gathered precisely at the time of the communication), certain forms of health information, 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 persons' names). Generally, this information would be gathered with or without consent of the data subject or with opt-in consent. Even if information could be collected without notice or consent, under current law it would be unlawful to do so under false pretenses, especially if the information would be used for a fraudulent purpose. Already under today's privacy laws, mandatory public display of what I classify as Tier II information is prohibited (as is shown by Social Security number laws).

The processing and use of Tier II information would hold fewer restrictions than for Tier I information. Nevertheless, the processing of this type of data would still have to be related to a legitimate purpose. The government would have an increased ability to obtain Tier II information, even without a warrant, as it can already do so under its Foreign Intelligence Surveillance Act[159] and USA PATRIOT Act[160] authority. As financial identity theft laws illustrate, fraudulent uses are already prohibited, even if information is gathered legally. In terms of time restrictions, Tier II information would have to be destroyed after the entity holding the data would no longer need it. Data security requirements for Tier II would not be as rigorous as for Tier I data. Although the main remedies for misuse of Tier II information would be civil, criminal penalties could be imposed as well. Given the sensitivity of Tier II information, as with Tier I information, liquidated and statutory damages could be available even if actual damages cannot be proven.

C. Tier III—Slightly Sensitive Information

Tier III would pertain to personally identifiable information of a lower privacy profile than the information in Tiers I and II. To the

159. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2006).

160. Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001, Pub. L. No. 107–56 (2001).

extent the information would be sensitive, Tier III would comprise of information that would be routed through a third party and, thus, there would be a decreased expectation of privacy. Examples of Tier III information would include connection records from telephone companies or Internet Service Providers (ISP) (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.[161] Consequently, these records would fall in Tier III.[162] This information could be gathered without consent and notice would typically not be required. Individuals could stop improper processing, but non-abusive processing should be permitted without consent. The government would have 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. Tier III information could not be gathered under false pretenses, especially if collected with fraudulent intent, which is shown by the recently enacted pretexting laws.

There would be general restrictions on data retention and destruction, but these requirements would not be as rigorous as those for Tier I and II and only reasonable steps would be necessary to secure and destroy data. Enforcement would be exclusively civil, though fraudulent uses could subject a person to criminal sanctions.

D. Tier IV—Non-Sensitive Information

Tier IV would contain personally identifiable, yet not truly private information. Examples of Tier IV information would include a

161. Pen registers are devices that disclose the telephone numbers that an individual called. These devices do not disclose the content of the communication.

162. United States v. Forrester, 495 F.3d 1041, 1048–49 (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.").

person's name, email address, telephone number, and address. Tier IV information could be collected without consent; however, if consent were necessary, an opt-out procedure could be available. While much of this information would be public, fraudulently gathering the information would not be permitted, particularly if doing so would misidentify the person requesting the information or further other misconduct. There would be a few restrictions on processing, but fraudulent acts and deception would not be permitted. Although data retention and destruction concerns would exist, there would be no extensive requirements on this type of data. Criminal enforcement could exist in limited circumstances, such as when other fraudulent acts would be undertaken using this type of information, but typically only civil remedies would be available 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. What follows is a sampling of statutes that track this principle, as well as the protection afforded by the classification of information into tiers.

A. The Computer Fraud and Abuse Act (CFAA)[163]

The Computer Fraud and Abuse Act (CFAA) was enacted to address the increasing number of computer crimes that were not covered under existing law.[164] Up until 1994, the CFAA only provided criminal penalties, but statutory amendments to the CFAA added civil remedies that can be used by companies to protect their network and recover damages for unauthorized access.[165] 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.[166] 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 tradi-

163. 18 U.S.C.A. § 1030 (West 2008).

164. *See* SERWIN, *supra* note 11, at ch. 3.

165. *Id.* § 3:1.

166. *Id.* § 3:18 (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001)).

tional 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.

Under the CFAA, criminal liability attaches when an individual "intentionally accesses a computer without authorization," or beyond the scope of any authorized use.[167] This applies regardless of whether the computer is owned by the government or the conduct involves interstate or foreign communication.[168] 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.[169] The wages of employees used to repair the damage can be considered when a court analyzes the $5,000 requirement.[170] 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.[171]

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 than 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.[172]

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,

167. 18 U.S.C.A. § 1030(a)(2) (West 2008).

168. *Id.* § 1030(a)(3).

169. *Id.* § 1030(a)(4); *see also* YourNetDating, Inc. v. Mitchell, 88 F. Supp. 2d 870 (N.D. Ill. 2000); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998).

170. *See, e.g.*, United States v. Middleton, 231 F.3d 1207, 1213–14 (9th Cir. 2000).

171. 18 U.S.C.A. § 1030(a)(5)(A)(i)–(iii) (West 2008).

172. *Id.* § 1030.

but neither damages for emotional distress or punitive damages are recoverable.[173]

The CFAA is a law that predominantly deals with what I define as Tier I information, because 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 is quite high and so is the level of penalties available for violation of this law, since both criminal and civil penalties, including fines, are available. The enforcement pattern of CFAA cases, even on the civil side, is 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[174]

California's concern over privacy led it to be one of the first states to enact an array of criminal statutes whose purpose 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.[175] California felt such a threat could not be tolerated in a free and civilized society.[176] Thus, the legislature passed the Invasion of Privacy Act in order to protect the right of privacy of the people of California.[177]

These restrictions are found in California Penal Code Section 631 *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 commu-

173. Garland-Sash v. Lewis, 1:05-cv-06827-WHP, 2007 WL 935013, at *2 (S.D.N.Y. March 26, 2007) (citing *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 n.33 (S.D.N.Y. 2001); Letscher v. Swiss Bank Corp., No. 94 Civ. 8277 (LBS), 1996 WL 183019, at *3 (S.D.N.Y. April 16, 1996)).

174. CAL. PENAL CODE § 630–637.9 (West 2009).

175. *Id.* § 630.

176. 18 U.S.C.A. § 1030(a) (West 2008).

177. CAL. PENAL CODE § 630 (West 2009).

nication while the [message] is in transit over a wire, line, or cable, or is being sent from or received at any place [in] the state."[178] California has also made it a crime to eavesdrop or record a confidential communication, which is defined as one whose circumstances "reasonably indicate that any party to the communication desires it to be confined to the parties thereto."[179] This does not include any communication that is made at a public gathering, in any legislative, judicial, executive or administrative proceeding that is open to the public, or any other instance in which the parties might reasonably expect that the communication would be overheard or recorded.[180]

California's law is an example of a law that regulates what I define as 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 practice.[181] The available criminal and civil penalties under this California law are consistent with my proposed treatment of Tier II information. In other portions of its Penal Code, California generally permits law enforcement to wiretap if a warrant is obtained,[182] which is also consistent with the proposed characteristics of Tier II information, since notice is not required to the target of the wiretap.

This law also contains restrictions similar to those that I recommend for Tier I information. 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."[183] Given the highly sensitive nature of this information, violation of this portion of the law is a crime.[184] However, consistent with Tier I, the law does "not apply to the lawful use of an electronic tracking device by a law

178. *Id.*

179. *Id.* § 632(c).

180. *See id.* § 633.

181. One California court permitted e-mail monitoring of employees where the employee had agreed to a monitoring policy as part of an employee handbook. TBG Ins. Serv. Corp. v. Super. Ct., 117 Cal. Rptr. 2d 155 (Cal. Ct. App. 2002).

182. CAL. PENAL CODE § 633 (West 2009).

183. *Id.* § 637.7(a).

184. *Id.* § 637.7(e).

enforcement agency," given the compelling need of law enforcement for this sensitive type of data.[185]

C. The Combined DNA Index System (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. The computer software program that processes and uses such an index is known as the Combined DNA Index System or CODIS.[186] The index is maintained by the Federal Bureau of Investigation (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.[187] The Attorney General[188] can "collect DNA samples[189] 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."[190] 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."[191] 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."[192]

This law governs what I describe as Tier I data, and while the governmental has certain rights to obtain this data, there are restrictions on the collection and retention of this 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 De-

185. *Id.* § 637.7(c).

186. 42 U.S.C.A. § 14135a(a)(3) (West 2009).

187. *Id.* § 14132(a)(1)(A)–(C).

188. This authority can be delegated to the Department of Justice, and other agencies that arrest, detain, or supervise individuals facing charges. *See id.* § 14135a(a)(1)(A).

189. "The term 'DNA sample' means a tissue, fluid, or other bodily sample of an individual on which a DNA analysis can be carried out." *Id.* § 14135a(c)(1).

190. *Id.* § 14135a(a)(1)(A).

191. *Id.* § 14135a(a)(1)(B).

192. *Id.* § 14135a(a)(2).

fense in accordance with 10 U.S.C.A. § 1565 (2000). The analysis must also be done "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, and:

> prepared by laboratories that—(A)[by] October 30, 2004, 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 (B) 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.[193]

Given the highly sensitive nature of this information (which I would classify as Tier I information), there are specific privacy requirements mandating that

> the results of DNA tests performed for a Federal law enforcement agency for law enforcement purposes may be disclosed only—(A) to criminal justice agencies for law enforcement identification purposes; (B) in judicial proceedings, if otherwise admissible pursuant to applicable statues or rules; and (C) 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.[194]

There are also expungement requirements that require the FBI to remove "promptly" the DNA analysis of a person in two circumstances.[195] 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 the 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."[196] If the original placement was due to "an arrest under the authority of the United States," the Director must strike out 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

193. *Id.* § 14132(b)(1)-(2)(A)-(B).
194. *Id.* § 14133(b)(1)(A)-(C).
195. *Id.* § 14132(d)(1)(A).
196. *Id.* § 14132(d)(1)(A)(i).

of a final[197] 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."[198] 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.[199]

D. Other Restrictions on Genetic Privacy

Alaska is one of many states that have placed strong restrictions on genetic privacy. It is generally illegal for a person to:

> collect a DNA[200] sample from an individual, perform a DNA analysis[201] 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.[202]

This restriction does not apply to DNA samples collected and analyzed for certain limited statutorily defined purposes; "for 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; for determining paternity; to screen newborns as required by state or federal law; [or] for the purpose of emergency medical treatment."[203]

---

197. "[A] court order is not 'final' if time remains for an appeal or application for discretionary review with respect to the order." *Id.* § 14132(d)(1)(C).

198. *Id.* § 14132(d)(1)(A)(ii).

199. *Id.* § 14135a(a)(5).

200. "'DNA' means deoxyribonucleic acid, including mitochondrial DNA, complementary DNA, and DNA derived from ribonucleic acid." ALASKA STAT. § 18.13.100(1) (2006).

201. As defined in the statute:

> "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.

Id. § 18.13.100(2).

202. *Id.* § 18.13.010(a)(1).

203. *Id.* § 18.13.010(b)(1)–(5).

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."[204] Given the concerns over this type of data, Alaska specifically stipulates 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]."[205] 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."[206] The law also provides for criminal penalties.[207]

This is another example of a law that covers what I define as Tier I information. As with the law that created CODIS, the Alaska law has 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. Moreover, Alaska made clear that a general medical authorization does not grant a right to any person to run DNA tests. Consistent with the proposed 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.[208]

E. Notice of Security Breach Laws

Notice of security breach laws have now swept the nation, with 44 states, Washington D.C., Puerto Rico 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.[209] Many states have

204. *Id.* § 18.13.010(a)(2).
205. *Id.* § 18.13.010(c).
206. *Id.* § 18.13.020.
207. As noted in the statute:

> 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].

Id. § 18.13.030(a).
208. *See, e.g.*, IDAHO CODE ANN. § 39-8303(1)(a)-(d) (2008).
209. For a complete discussion of these laws, see SERWIN, *supra* note 11, at ch. 21.

restricted notice to situations where there is unencrypted data at issue, but this is not always the case. Moreover, consistent with the proposed tiered approach to privacy protection, only certain breaches of security (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 for two reasons. First, while there are breaches that cause damage to consumers, the vast majority do not. Although some states 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. The tort concept of damages is not the basis of the security breach laws and the model instead is based upon enforcement related to the sensitivity of the data and not whether there was damage.

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.[210] As 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.[211]

Section 1798.82 applies to instances of data security breaches that involve a consumer's personal information.[212] The statute originally defined personal information as either an individual's first name or first 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.[213] However, recognizing the inherent sensitivity of other types of what I define as Tier I information, California recently amended the definition to include "medical information"[214] as well as health in-

210. CAL. CIV. CODE § 1798.82 (West 2008).

211. This law impacts such companies because it attempts to regulate companies that gather information regarding California citizens, irrespective of the corporate headquarters. *Id.* § 1798.82.

212. *Id.* § 1798.82(b).

213. *Id.* § 1798.82(e).

214. 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." *Id.* § 1798.82(f)(2).

surance 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.[215] 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.[216] 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.[217] 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 pertain to information whose sensitivity profiles would place it in my proposed Tiers I and II. The California data security breach law covers what I define as Tier I and II information, because 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 Tiers I and II. One observation about these laws, which in essence require the party that has suffered a breach to mitigate the risks of the breach, is that the duty to mitigate is placed upon the party that would be a defendant in a civil suit and not the plaintiff, who typically would have the duty to mitigate its damages. 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

215. *Id.* § 1798.82(a)–(b).
216. *Id.* § 1798.82(a).
217. *Id.*

we take for granted.[218] 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 involving computerized data requires notice. This also is consistent with Privacy 3.0's analysis.

F. The Videotape Privacy Protection Act[219]

The Videotape Privacy Protection Act is a Federal law that governs the disclosure of certain consumer video records and, similar to the pretexting laws, it resulted from a highly publicized privacy incident.[220] It is a violation of Federal law for any video tape service provider to knowingly disclose personally identifiable information[221] concerning any consumer.[222]

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.[223] 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."[224]

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."[225] The subject matter of video tapes may be disclosed

---

218. 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.

219. 18 U.S.C.A. § 2710 (West 2009).

220. In this incident, a reporter sought and obtained Judge Robert Bork's video rental records during his confirmation hearings for the Supreme Court. *See* Dirkes v. Borough of Runnemede, 936 F.Supp. 235, 239 (D.N.J. 1996) ("The impetus for enacting the measure arose as a result of Judge Robert Bork's 1987 Supreme Court nomination battle, during which a Washington, D.C. newspaper obtained a list of 146 video tapes the Bork family had previously rented from their neighborhood store.").

221. "'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) (West 2009).

222. *Id.* § 2710(b)(1); *see also* SERWIN, *supra* note 11, at ch. 23.

223. 18 U.S.C.A. § 2710(b)(2)(A)–(B) (West 2009).

224. *Id.* § 2710(b)(2)(C).

225. *Id.* § 2710(b)(2)(D).

only "if the disclosure is for the exclusive use of marketing goods and services directly to the consumer."[226] There are also other permitted disclosures, including with a court order.[227]

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 attorney's fees and costs, and any other preliminary or equitable relief.[228]

This law is an example of a law that covers what I label as 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[229]

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[230] 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 a number of issues regarding the collection and disclosure of personally identifiable information.[231] There are also restrictions on the collection and disclosure of information, though exceptions exist for certain legitimate business purposes.[232]

Similarly to other laws that cover what I classify as Tier II information, the Cable Privacy Act provides a range of remedies which

226. *Id.* § 2710(b)(2)(D)(ii).
227. *Id.* § 2710(b)(2)(E)–(F).
228. *Id.* § 2710(c)(1)–(2).
229. 47 U.S.C.A. § 551 (West 2009).
230. "'[O]ther 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." *Id.* § 551(a)(2)(B).
231. *Id.* § 551(a)(1).
232. *Id.* § 551(c)(2)(A).

include attorney's fees as well as actual, liquidated and punitive damages.[233]

This is another example of a law covering information which my proposal would place in Tier II. This Act contains strong limitations 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.[234]

H. Credit Freeze Laws

Credit or security freezes permit consumers to place restrictions upon the use and disclosure of their consumer report.[235] 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 also restricts the consumer's ability to obtain credit, unless the customer temporarily lifts the freeze. 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 (since one of the main purposes of notice is to alert consumers of potential risks to their credit) 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. As with the notice of security breach laws, there are statutory penalties, not just damages, which 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[236] be placed on his or her consumer credit

---

233. Any affected person may bring an action in federal court seeking "actual damages but not less than 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." *Id.* § 551(f)(1)–(2).

234. For a complete discussion of these state laws, see SERWIN, *supra* note 11, ch. 24.

235. For a discussion of credit freeze laws, see SERWIN, *supra* note 11, ch. 10.

236. As noted in the statute:

report[237] and a consumer credit reporting agency that receives a written request from a consumer, as referenced above, must, if the statutory prerequisites are met, place a security freeze on the consumer's consumer credit report no later than four business days after receiving the written request.[238]

> 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.[239]

Given the perceived need to protect consumers, 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

---

> 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) (McKinney 2009).

237. "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." *Id.* § 380-a(l).

> (1) 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.
>
> (2) 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.

Id. § 380-a(c)(1)-(2).

238. *Id.* § 380-t(b).

239. *Id.* § 380-t(j).

on certain limited circumstances. While a freeze does apply to many entities, there are many exemptions to these laws.[240]

The New York credit freeze law seems to cover what I classify as 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's 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 relate to what I identify as Tier II information[241] because they pertain to reasonably sensitive information that is used fraudulently. Violations of these laws can result in both criminal and civil penalties.

Delaware law provides a good example of identity theft laws. A person commits identity theft in Delaware "when the person knowingly or recklessly obtains, produces, possesses, uses, sells, gives or transfers personal identifying information[242] belonging or pertain-

---

240. Certain entities are not required to place a security freeze on a consumer credit report, including:

> (2) 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;
>
> (3) 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.

Id. § 380-t(p)(1)–(3).

241. *See* SERWIN, *supra* note 11, at ch. 19.

242. As noted in the statute:

> "[P]ersonal 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

ing to another person without [consent] and with intent to use the information to commit or facilitate any other crime."[243] 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."[244]

Identity theft in Delaware is a felony.[245] 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" if the defendant is found guilty of identity theft.[246]

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[247] . . . without first obtaining that individual's consent."[248] This crime is a felony

---

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) (2007).

243. *Id.* § 854(a).

244. *Id.* § 854(b).

245. *Id.* § 854(d).

246. *Id.* § 854(e).

247. As noted in the statute:

> "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. § 817.568(1)(f) (2007).

248. *Id.* § 817.568(2)(a).

punishable by a prison term of not greater than five years and a fine of not greater than $5,000 with additional penalties for habitual offenders and higher levels of damages.[249]

Florida's law demonstrates an inherent weakness of common law based theories with tort enforcement—misuse of deceased individual's personally identifiable information. Typically a lawsuit based upon tort theories requires a living plaintiff, but identity theft can occur with deceased individuals. Florida has addressed this issue via statute and has made it a crime if any person "willfully and fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning a deceased individual [thus committing] the offense of fraudulent use or possession with intent to use personal identification information of a deceased individual."[250]

J. Restrictions on Social Security Numbers

Social Security number laws also pertain to what I describe as Tier II information. Arizona's law is discussed below.[251] Arizona has made it illegal, as of January 1, 2005, for a person or entity to:

1. Intentionally communicate or otherwise make an individual's social security number available to the general public.
2. 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.
3. 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.
4. Require the use of an individual's social security number to access an internet web site, unless a password or unique personal identification number or other authentication device is also required to access the site.
5. 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

249. *Id.* §§ 775.082–775.084, 817.568(2)(a)–(b), (6)–(7).

250. *Id.* § 817.568(8)(a).

251. See SERWIN, *supra* note 11, at ch. 23 for a complete discussion of these laws.

> state or federal law requires the social security number to be on the document to be mailed.[252]

Arizona's law covers what I classify as Tier II information, and it imposes broad restrictions on the disclosure of Social Security numbers. These limitations are not absolute, particularly in the context of preexisting use. However, consistent with the characteristics of Tier II information, even with the preexisting use, the consumer can elect to stop that use. 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 will cover what I describe as Tier III information. 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, and mainly this relates to the gathering of telephone records and financial information, though certain states, including Illinois, have expanded the definition of covered information.[253] Illegal pretexting can be improper depending on the type of data, the type of person seeking it, and the purpose of the request.

The federal government enacted the Telephone Records and Privacy Protection Act of 2006, which governs pretexting.[254] It is a crime for any person in interstate or foreign commerce to

252. ARIZ. REV. STAT. ANN. § 44-1373(A)(1)–(5) (2008).
253. 72 ILL. COMP. STAT. ANN. 5/18G-14(a) (West. 2009).
254. 18 U.S.C.A. § 1039 (West 2009).

knowingly and intentionally obtain, or attempt to obtain, confidential phone records information[255] of a covered entity[256] by—

(1) making false or fraudulent statements or representations to an employee of a covered entity;

(2) making [a] false or fraudulent statements or representations to a customer of a covered entity;

(3) providing a document to a covered entity knowing that [the] document is false or fraudulent; or

(4) 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.[257]

It is also illegal, unless otherwise permitted by law, to "knowingly and intentionally sell, transfer, or attempt to sell or transfer, confidential phone record information of a covered entity, without

---

255. As noted in the statute:

> 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 by a customer 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.

Id. § 1039(h)(1).

256. As noted in the statute:

> "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. § 153); and (B) includes any provider of IP-enabled voice service." *Id.* § 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.

Id. § 1039(h)(4).

257. *Id.* § 1039(a).

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."[258] This is also a crime punishable by a fine, a prison term of not more than ten years, or both.[259] 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 law that regulates what I label as Tier III information. While there are criminal penalties involved, a violation of this law only occurs if the records were gathered in a fraudulent way, or if 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. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)[260]

CAN-SPAM presents a clear example of a law that would fall within the proposed Tier IV law.[261] Congress passed the CAN-SPAM Act in reaction to certain state e-mail laws, California's in particular.[262] These state laws went far beyond what the federal government was willing to do, so CAN-SPAM was passed with the goal of preempting (and in essence nullifying) the troublesome portions of state law.[263] 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.[264] Despite this perceived shortcoming, CAN-SPAM has increased the FTC's ability to stop spam.[265] States at this point seem to be taking a back seat to the

258. *Id.* § 1039(b)(1).

259. *Id.*

260. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C.A. §§ 7701–7713 (West 2009).

261. See SERWIN, *supra* note 11, at chs. 7–8 for a discussion of CAN-SPAM and state email laws.

262. CAL. BUS. & PROF. CODE § 17529.1 (West 2008).

263. 15 U.S.C.A. § 7701(a)(11) (West 2003).

264. 15 U.S.C.A. § 7704(a)(5)(b) (West 2003).

265. 15 U.S.C.A. § 7706(a) (West 2003).

FTC on these issues, though state law-based lawsuits relating to unsolicited e-mail still occur.[266]

Given the judgment by Congress that a person's email address did not justify the level of protection afforded by state law, CAN-SPAM in essence placed three main requirements on most entities that send advertisements through e-mail. First, they must have a "clear and conspicuous identification that the message is an advertisement or solicitation."[267] 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.[268] Third, each commercial e-mail must contain a valid physical postal address for the sender.[269] 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.[270]

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

This law deals with proposed Tier IV information. Consumers can object to receiving e-mails, but it is not illegal for a person to send unsolicited emails. Also, 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 of a

266. *See, e.g.*, Omni Innovations, LLC v. Impulse Mktg. Group, Inc., No. C06-1469MJP, 2007 WL 2110337 (W.D. Wash. July 18, 2007); Gordon v. Virtumundo, Inc., No. 06-0204-JCC, 2007 WL 1459395 (W.D. Wash. May 15, 2007); Phillips v. Netblue, Inc., No. C-05-4401 SC, 2006 WL 3647116 (N.D. Cal. Dec. 12, 2006); ASIS Internet Services v. Optin Global, Inc., 65 Fed. R. Serv. 3d 404 (N.D. Cal. 2006).

267. 15 U.S.C.A. § 7704(a)(5)(A)(i) (West 2003).

268. *Id.* § 7704(a)(3)(A)–(B), (a)(5)(A).

269. *Id.* § 7704(a)(5)(a)(iii).

270. *Id.* §(a)(5)(B).

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 discussed in this Article is when the CFAA was amended several years ago. In order to prove one type of claim under the CFAA the plaintiff must show "loss."[271] Previously, there was no requirement that an electronic system be damaged, but the recent amendment 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. Similarly, 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, no loss, as have other courts.[272] However, many other courts have struggled with this requirement and reached inconsistent results. In *Spangler*, the District Court for the Northern District of Indiana also recently assessed the damage element for a Section 1030(a)(5) claim in the context of alleged misconduct by an attorney as she departed her former employer.[273] In this case, the plaintiff alleged that the defendant, a partner at plaintiff's law firm, took proprietary information, including client lists and e-data files, before her departure from the firm and as

271. 18 U.S.C.A. § 1030(a)(5)(C) (West 2008).

272. *See* Therapeutic Research Faculty v. NBTY, 488 F. Supp. 2d 991 (E.D. Cal. 2007) (citing Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000)) (holding that a claim could be stated under the CFAA against a party that exceeded authorized use of a password and thereby obtained additional access to licensed materials); *see also* PharMerica, Inc. v. Arledge, No. 8:07-cv-00486-T-26MAP, 2007 WL 865510, at *1 (M.D. Fla. Mar. 21, 2007) (holding that employer had demonstrated likelihood of success on CFAA claim where an employee that downloaded confidential information to use with a competitor and deleted files and records related to the downloading); H & R Block E. Enters., Inc. v. J&M Sec., LLC, No. 05-1056-W-DW, 2006 WL 1128744, at *4 (W.D. Mo. Apr. 24, 2006); Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004); Pacific Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188 (E.D. Wash. 2003).

273. Spangler, Jennings & Dougherty, P.C. v. Mysliwy, 2:05-cv-108, 2006 U.S. Dist. LEXIS 39602, at *1 (N.D. Ind. Mar. 31, 2006).

part of her plan to set up a competing law firm. The plaintiff moved for summary judgment on its CFAA claim which the court ultimately denied, noting that while the plaintiff argued 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 would support a finding of qualified losses under Section 1030(a)(5).[274] Again other courts have followed this line of reasoning as well.[275]

The interruption in service requirement continues to befuddle courts. For example, in *P.C. of Yonkers*,[276] 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, as they had not demonstrated any "loss" under Section 1030(a)(5)(B)(1).[277] The *P.C. Yonkers* court examined *Nexans Wires S.A. v. Sark-USA, Inc.*[278] and *Resdev*[279] and concluded that these cases made a distinction between costs incurred as a result of an incident and lost revenue or other consequential damages.[280] The court noted 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."[281] The court concluded that the

274. *Id.* at 13; *see also* Resdev, LLC v. Lot Builders Ass'n, No. 6:04-cv-1374-Orl-31DAB, 2005 U.S. Dist. LEXIS 19099, at *12 (M.D. Fla. 2005) (explaining that the CFAA requires some finding of "diminution in the completeness or usability of data or information on a computer system"); Moulton v. VC3, No. 1:00-CV-434-TWT, 2000 U.S. Dist. LEXIS 19916, at *20 (ND. Ga. 2000) (disallowing investigative costs as damage under the CFAA where alleged incident did not result in "structural" damage to the network).

275. Cenveo Corp. v. CelumSolutions Software GMBH & Co KG, 504 F. Supp. 2d 574 (D. Minn. 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*, 2006 U.S. Dist. Lexis 39602, at *20 (stating that 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).

276. No. 04-4554 (JAG), 2007 WL 708978, at *1 (D. N.J. Mar. 5, 2007).

277. *Id.* at *4.

278. 166 Fed. Appx. 559 (2d Cir. Feb. 13, 2006).

279. *Resdev, LLC*, 2005 U.S. Dist. LEXIS 19099, at *12.

280. *P.C. of Yonkers, Inc.*, 2007 WL 708978, at *4 ("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." (internal citations and quotations marks omitted)).

281. 18 U.S.C.A. § 1030(e)(11) (West 2008).

"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 . . ."[282] Thus, the court read the definition of loss to have two different components, the first 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 that includes lost revenue, incurred costs, or other consequential damages that result from an interruption of service.[283] Under this definition, the court concluded that the plaintiffs had stated a claim under the CFAA.[284] It is notable that the plaintiffs in this matter never alleged either damage or interruption of service, but rather argued that they had suffered "substantial losses in excess of $5,000.00, including but not limited to losses sustained in responding to defendants' actions, investigating defendants' actions and taking remedial steps to prevent defendants' further actions."[285] 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*.[286] In this case, the plaintiff alleged that its former employees took proprietary and trade secret information from their former employer, L-3, in the form of emails and an external drive containing an extensive number of confidential files.[287] The plaintiff argued that the defendants used this information to compete with L-3 in an effort to obtain government contracts.[288] Although this court relied upon the same cases as the *P.C. Yonkers* court, it reached a different conclusion.[289] In fact, this court created a two-pronged definition of loss, one portion of which

282. *P.C. of Yonkers, Inc.*, 2007 WL 708978, at *4–5.

283. *Id.*

284. *Id.* at *5.

285. *Id.*

286. No. 2:06-cv-00279-MLV-SS, 2007 WL 756528, *1 (E.D. La. Mar. 8, 2007)

287. *Id.* at *2–3.

288. *Id.* at *2.

289. This court concluded, based on *Nexans*, that a plaintiff must allege either damage to a computer or an interruption of service to show loss under Section 1030(g). *Id.* at *4 (citing Civil Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd., 387 F. Supp. 2d 378, 381–82 (S.D.N.Y. 2005); Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d. 468, 478 (S.D.N.Y. 2004)) ("[C]osts not related to computer impairment or computer damages are not compensable under the CFAA.").

requires damage to a computer, and one that requires an interruption of service. The court concluded that a CFAA claim could not be stated because the only allegation was theft of trade secrets and confidential information and the resulting harm was misuse of the information to compete, without a showing of damage to a computer or an interruption of service.[290]

The confusion created by the insertion of the interruption in service requirement demonstrates the need for a cohesive theory of privacy based on factors related to the sensitivity of the data, not impairment of a network. If the concern with the CFAA that led to the amendment inserting the interruption in service element was a worry that too many CFAA claims would be brought if the threshold was only $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.

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 whether the common law should 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 that 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.

290. *Id.*