August 7, 2010

What’s Privacy Got to Do, Got to Do with It: Why Information Should Drop Privacy and Seek Legal Love on Its Own Terms

Christopher E Paxton, University of San Francisco
What's Privacy Got to Do, Got to Do with It\textsuperscript{1}: Why Information Should Drop Privacy and Seek Legal Love on Its Own Terms

Christopher Paxton

\textsuperscript{1} A reference to Tina Turner, \textit{What’s Love Got To Do With It}, on Private Dancer (Capitol Records 1984).
# Table of Contents

I. Introduction ............................................................................................................................ 1

II. The State of the Relationship ............................................................................................... 3
    A. Torts ................................................................................................................................. 3
    B. Statutes ............................................................................................................................. 5
    C. Constitutional Approaches ............................................................................................. 6
    D. Market Approaches ......................................................................................................... 7

III. Problems in Paradise ........................................................................................................... 8
    A. Tort Problems .................................................................................................................. 9
    B. Statutory Problems ......................................................................................................... 11
    C. Constitutional Problems ............................................................................................... 13
    D. Market Problems .......................................................................................................... 14

IV. Blame Privacy ...................................................................................................................... 18

V. The Case for Information ...................................................................................................... 21
    A. How Protecting Information Protects Privacy ............................................................. 21
    B. Sui Generis Protection of Information ........................................................................... 24
    C. As Distinguished from Other Privacy-as-Intellectual-Property Regimes ...................... 26
    D. Benefits and Drawbacks ............................................................................................... 27

VI. Conclusion: Why Privacy has Such a Bad Rap ................................................................. 30
I. Introduction

What’s Privacy but a visceral reaction? Warren and Brandeis had such a reaction to the advent of the “snap camera” and successfully articulated the reaction in their landmark paper. Such reactions have come about with the emergence of almost every new technology: the computer, the telephone, the Internet, etc. And with each technological step came a cry from the hills that Privacy as we know it is coming to an end. To call Privacy a visceral reaction is not meant to insult Privacy or its advocates. As demonstrated in the cases, the harm from privacy invasions can be difficult to articulate unless one uses emotional terms: hurt feelings, worry, anguish, etc. This emotional core may explain why Privacy, standing alone, has had a relatively difficult time gaining the full legal protection it deserves.

Perhaps as a way to overcome this deficiency, Privacy at some point teamed up with Information to form the legal field of Information Privacy. This alliance seems quite natural at first glance. The event that often causes one’s Privacy to be breached is the revealing of information that one does not want revealed. Information and Privacy are similar in that they intersect so many legal disciplines. Information is discussed in contract law, property, intellectual property, torts, etc. Privacy is discussed in contract law, property, constitutional law, torts, etc. Many of the federal privacy statutes are written to address the disclosure and exchange of information. Doctrinally speaking, however, Information and Privacy make for strange bedfellows. The nature of Information’s intersection with the above mentioned areas of law differs greatly from Privacy’s intersection. Information is included in these disciplines in a concrete way. Privacy, on

---

5 E.g., Pisciotta v. Old Nat’l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007).
the other hand, is analogized to these disciplines out of legal necessity. In order to make the case for Privacy’s protection, Warren and Brandeis drew from other fields of law to show that in some deep way, Privacy was already protected at common law. Many scholars have attempted to pin down the precise nature of Privacy, arguably with limited success. With Information, it is not necessary to make expansionist arguments. Information fits in naturally as property and intellectual property. The same cannot be said for Privacy, hence all of the analogies to protection of other things such as property and data security. In linking Privacy with Information, perhaps the hope was that Privacy’s association with Information would make Privacy more legally concrete. However, Information Privacy has adopted more of the deficiencies of Privacy than the advantages of Information.

The extent of these deficiencies and how they can be overcome is the topic of this paper. More precisely, this paper aims to demonstrate that the best, most comprehensive way to protect Privacy is to focus on Information by removing the privacy rhetoric from the conversation and focusing on Privacy’s legally redressable aspects as embodied by Information. The paper will give a brief overview of the state of Information Privacy protection in the United States, including an analysis of its successes and failures. Next, arguments will be presented attributing Information Privacy’s failures to Privacy and its successes to Information. Thirdly, the nature of information protection and how it can account for privacy concerns will be explored. The paper will conclude with thoughts as to why privacy protection is so elusive. Is there something intrinsic to Privacy that makes it unpopular with the other legal disciplines? Perhaps Privacy is simply bad at relationships.

---

8 See Warren & Brandeis, supra note 3, at 197-206.
9 See, Solove & Schwartz, supra note 2, at 39-59.
II. The State of the Relationship

Perhaps as proof of Warren & Brandeis’ belief that privacy protection is deeply rooted in America’s legal system, or as evidence of its failure to win legal recognition in its own name, information privacy protection has taken on just about every legal form imaginable.\(^{10}\) There are the privacy torts for civil litigation; a host of federal and state, civil and criminal statutes aimed at particular industries; federal and state constitutions; contractual agreements and privacy policies; international treaties and guidelines; and Federal Trade Commission (“FTC”) regulations.

A. Torts

As formulated by Prosser\(^{11}\), privacy is divided into four torts, recognized in varying degrees by courts. First, there is intrusion upon seclusion, requiring a highly offensive, intentional intrusion upon the solitude or seclusion of another’s private affairs or concerns.\(^{12}\) It is typically applied to journalists or the paparazzi gathering information about an individual without that individual’s consent or approval. Taping phone conversations of a well-known politician\(^{13}\) is an example of actionable conduct. The reporting practices used in the recent Tiger Woods media storm could give rise to intrusion upon seclusion if reporters were, say, hiding out in Mr. Woods’ basement rather than lurking outside his home, talking to friends and acquaintances, and making inferences.

Public disclosure of private facts involves the disclosure or publication of private information that is not newsworthy.\(^{14}\) As with intrusion upon seclusion, the typical situation involves an individual seeking remedy for the media’s highly offensive actions. Examples include photo-

\(^{10}\) A third possibility is that this is an attempt at comprehensive privacy protection.
\(^{12}\) *Id.* at 389-92.
\(^{14}\) Prosser, *supra* note 11, at 392-98.
graphing an unsuspecting woman while a jet of air reveals what her skirt was trying to hide\textsuperscript{15} and revealing the gender history of an elected student body president.\textsuperscript{16} Related, but distinct, is the tort of false light.\textsuperscript{17} The tort is related to public disclosure in that it requires publication by the tortfeasor.\textsuperscript{18} It is distinct in that the publication does not involve the truth.\textsuperscript{19} False light is perhaps the most criticized of the privacy torts.\textsuperscript{20}

Finally, there is misappropriation of one’s name or likeness for the tortfeasor’s use or benefit.\textsuperscript{21} The classic misappropriations case is similar to an action for trademark infringement: the tortfeasor uses a famous person’s name or likeness, the individual’s “trademark,” for the tortfeasor’s commercial benefit, e.g. by creating an impression that the famous person sponsors or is in some other way connected with the goods or services being offered for sale. Misappropriation has been codified in state laws, most notably in New York\textsuperscript{22} and California.\textsuperscript{23}

There is also the occasional allegation of negligence, provided that the tortfeasor had a duty to protect the plaintiff’s privacy. In one case, the court found a duty where the harm resulting from defendant’s disclosure was foreseeable, creating a “special circumstance”.\textsuperscript{24} Credit card issuers have also been found to have a duty to verify the accuracy and authenticity of credit applications.\textsuperscript{25}

\textsuperscript{15} Daily Times Democrat v. Graham, 276 Ala. 380 (1964).
\textsuperscript{16} Diaz v. Oakland Tribune, Inc., 188 Cal. Rptr. 762 (Cal. Ct. App. 1\textsuperscript{st} Dist. 1983).
\textsuperscript{17} Prosser, supra note 11, at 398-401.
\textsuperscript{18} See id. at 399-400.
\textsuperscript{19} Id. at 400.
\textsuperscript{20} See, e.g., Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235-36 (Minn. 1998).
\textsuperscript{21} Prosser, supra note 11, at 401-07.
\textsuperscript{22} N.Y. Civ. Rights Law §§ 50-51 (McKinney 2009).
\textsuperscript{25} Wolfe v. MBNA America Bank, 485 F. Supp. 2d 874, 882 (W.D. Tenn. 2007).
B. Statutes

In addition to statutes that codify the privacy torts, there are statutes that require a third party to protect consumers’ privacy where otherwise there would be no duty—common law, contractual or otherwise—to do so. The network of statutory protection is sectoral in nature, applying to particular industries engaged in particular activities. The industries covered and protections afforded are too numerous to list. Here, a brief overview of the network is provided, organized according to the industry covered.

On the Internet, the protection is two-fold, regulating disclosure and regulating unauthorized access. The Children’s Online Privacy Protection Act falls into the former category. The statute limits the circumstances under which websites can collect information about children and gives parents the right to know what information is being collected about their children. The Electronic Communications Privacy Act falls into the latter category. In particular, the Wiretap Act addresses the interception of communications while in transit. The Stored Communications Act addresses access to stored communications.

On television and in the video store, there are the Cable Communications Policy Act and the Video Privacy Protection Act. Both regulate the disclosure of consumers’ viewing habits. In the library, many states have enacted statutes prohibiting the disclosure of library records. At the bank, the Gramm-Leach-Bliley Act governs the collection and disclosure of ac-

---

26 Solove & Schwartz, supra note 2, at 794.
28 Id. § 6502(a)(1), (b)(1)(A).
29 Id. § 6502(b)(1)(B).
31 Id. §§ 2510-2522.
32 Id. §§ 2701-2709.
35 Solove & Schwartz, supra note 2, at 573.
count holders’ information. Concerning virtually every financial transaction, the Fair Credit Reporting Act\(^{37}\) governs the creation of, maintenance of, and access to credit reports. At the hospital, the Health Insurance Portability and Accountability Act\(^{38}\) (“HIPAA”) both facilitates the free exchange of health information – with the goal of allowing employees to change jobs without facing gaps in coverage – and limits disclosure and use for non-health related purposes.

Many states have passed their own sectoral privacy protections, at least where federal statutes have not preempted state action. Many states have enacted health privacy protections.\(^{39}\) States have also adopted data breach notification laws.\(^{40}\) In California, for example, companies are required to notify California residents if their “personal information was, or is reasonably believed to have been, acquired by an unauthorized person”\(^{41}\) unless notification would hinder an ongoing investigation.\(^{42}\)

C. Constitutional Approaches

The constitutional privacy conversation is multifaceted. The 4\(^{th}\) Amendment addresses privacy invasions by law enforcement and other state actors. The 14\(^{th}\) Amendment has been interpreted to address decisional privacy, typically in terms of liberty and substantive due process.\(^{43}\) The 1\(^{st}\) Amendment has also been cited as a source of privacy, particularly with regards to the right of anonymous association.\(^{44}\) The Supreme Court has used the 9\(^{th}\) Amendment as a way

---

\(^{39}\) Solove & Schwartz, supra note 2, at 429-31.
\(^{40}\) Id. at 826-27.
\(^{41}\) Cal. Civ. Code § 1798.82(a).
\(^{42}\) Cal. Civ. Code § 1798.82(c).
\(^{44}\) E.g., NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).
to protect non-enumerated rights such as privacy.\textsuperscript{45} Even the 5\textsuperscript{th} Amendment has been argued as a source of privacy.\textsuperscript{46} The Supreme Court has specifically addressed information privacy in the health context\textsuperscript{47} and seems to have settled on deciding the existence of a privacy right on a case-by-case basis by balancing the intrusion against the government’s interests while also taking into account safeguards in place.\textsuperscript{48} At the state level, the constitutions of Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington explicitly protect privacy.\textsuperscript{49}

D. Market Approaches

Privacy policies are perhaps the most popular market tool. Even when not explicitly required by statute, many companies have created detailed privacy policies and are members of trade groups dedicated to protecting privacy. This is especially true of Internet companies like Google\textsuperscript{50}, Yahoo\textsuperscript{51}, and Facebook\textsuperscript{52}, and of online retailers such as Best Buy, NexTag, and Snapfish.\textsuperscript{53} The popularity and practices of social networking sites have made online privacy concerns even more prominent. Facebook, for example, has been in news recently for updating its privacy protections.\textsuperscript{54}

\textsuperscript{45} Erwin Chemerinsky, Constitutional Law 817 (Erwin Chemerinsky et al. eds., Aspen Publishers 2d ed. 2005).
\textsuperscript{48} See id. at 600-604.
The market also offers various products and services that can be used to affirmatively protect consumers’ privacy. Many web browsers allow users to select a privacy mode\textsuperscript{55} whereby the user’s browsing history and other data is not stored by the browser.\textsuperscript{56} Companies such as LifeLock and Privacy Guard provide services that prevent and provide notice of identity theft, and allow the consumer to actively monitor her credit. Domains by Proxy and similar companies allow domain name owners to register anonymously rather than making their contact information available to anyone willing to conduct a WHOIS search.

Apart from self-regulation and market offerings, the FTC also regulates privacy in the private sector. The typical situation involves a company deviating from its privacy policy without informing the consumer. The FTC views such discrepancies as deceptive practices or unfair acts.\textsuperscript{57} The FTC’s enforcement tools include civil penalties and cease and desist orders.\textsuperscript{58}

III. Problems in Paradise

Despite this broad network of information privacy protections, establishing comprehensive protection has proven to be an elusive task at best. Within the current system, there are too many exceptions, too many hurdles to recovery, and too many gaps in protection. Perhaps most endemic is the all-or-nothing approach to privacy. Once something has entered the public domain, it cannot be recaptured.\textsuperscript{59} There does not seem to be a concept of limited disclosure in in-

\begin{itemize}
\item Privacy mode is called private browsing in Safari and Firefox, incognito mode in Chrome, and InPrivate Browsing in Internet Explorer.
\item Solove & Schwartz, supra note 2, at 776.
\item See, e.g., Sidis v. F-R Publ’g Corp. 113 F.2d 806 (2d Cir. 1940).
\end{itemize}
formation privacy law. Small chinks in one’s privacy armor can lead to non-remediable inva-
sions.  

Related to the all-or-nothing approach is the third-party doctrine. Once an individual
communicates information to a third party, she assumes the risk that the third party will further
disclose the information, either to the state or to other private parties. The Supreme Court has
held on several occasions that getting information about an individual from a third party does not
violate the individual’s Fourth Amendment rights.

A third problem with the current network of protection is the difficulty of establishing a
legally cognizable harm. All too often, courts have refused to grant a remedy because the injury
is merely speculative, only involves hurt feelings, or is the result of mere exposure to harm
without suffering. Refusing relief on these bases is ironic considering that privacy law was spec-
cifically designed to remedy that which is often felt only in speculative, emotional, and vulner-
able terms.

A. Tort problems

The Third Party Doctrine is particularly damning to privacy tort claims. If the alleged
tortfeasor attempts to solicit information about the plaintiff from the plaintiff’s friend, there is no
intrusion upon seclusion. One’s solitude or seclusion is not invaded by talking to a confidant as
one has taken the risk that the confidant will reveal one’s confidences.

---

60 See, e.g., Florida v. Riley, 488 U.S. 445, 450-51 (1989); The Florida Star v. B.J.F., 491 U.S. 524, 546 (White, J.,
dissenting).
63 E.g., Laird v. Tatum, 408 U.S. 1, 12-14 (1972).
65 E.g., Pisciotta v. Old Nat’l Bancorp, 499 F.3d 629, 638-39 (7th Cir. 2007).
66 See Warren & Brandeis, supra note 3, at 205-07.
Concerning the public disclosure tort in particular, courts’ deferential view of the last element, whether the fact is newsworthy, is problematic. Courts usually let the press decide what is newsworthy or look to the customs and conventions of the community, which are essentially deference to the media and the public. The tests boil down to this: If it’s published and people are reading it, it must be newsworthy. Getting any more involved might require courts to make decisions about what is gossip and what is news. However, a normative inquiry is exactly what is required in determining newsworthiness. The phrase “of legitimate public concern” has both a subjective and objective element. First, the private fact must be of actual public concern, i.e. whether the public is actually interested. Second, that concern must be legitimate or, in other words, objectively reasonable. The European Court of Human Rights has taken this approach, defining newsworthy information as that which “contributes to a debate of general interest” and interpreting the phrase to exclude such things as photos of one’s private life.

American information privacy law could further learn from the European model by fully adopting the breach of confidence tort, which is currently recognized only in certain types of fiduciary relationships. Recognition of the tort would import the concept of limited disclosure into information privacy law. The all-or-nothing approach would have to be rethought, having profound and positive impacts on the American privacy torts. Recognizing the tort would import the concept of privacy as human dignity, something that is prevalent in European privacy law. The tort’s adoption would also create a direct conflict with the Third Party Doctrine. One cannot

---

68 Solove & Schwartz, supra note 2, at 124-25.
70 Id. at 26-27.
71 Solove & Schwartz, supra note 2, at 139.
be assumed to have assumed the risk of third party disclosure if the law is willing to impose a duty of non-disclosure on that third party.

B. Statutory Problems

As discussed above, the network of statutory regulation is very complex, applying activity by activity, industry by industry. In addition to regulating disclosure, most statutes contain numerous exceptions as to which entities are covered, what information is covered, and with which entities information may be shared. Take HIPAA as an example. Generally, the regulations require patient authorization for the sharing and use of medical information for marketing purposes.73 However, because of an exception, the health service provider can use medical information to market its own products to its customers.74 Disclosure to law enforcement, to state health departments for health emergencies, and for judicial and administrative proceedings is also excepted.75

The statutes and accompanying regulations create a legal obstacle course for companies engaged in several types of activities covered by different information privacy statutes. For example, a cable company that provides Internet access must abide by at least the Cable Communications Privacy Act76, the Children’s Online Privacy Protection Act77, the Fair Credit Reporting Act78, and the Electronic Communications Privacy Act.79 It must be admitted that large companies are subject to all sorts of regulations. However, the necessity of regulation does not take

---

74 45 C.F.R. § 164.501 (“Marketing means: To make a communication about a product or service…unless the communication is made to describe a health-related product or service…that is provided by…the covered entity making the communication[.]”).
75 45 C.F.R. § 164.512 (2009).
away from the difficulty of compliance created by statutory and regulatory complexity. The complexity of statutory regulation is due at least in part to its sectoral coverage. Statutes are written to cover particular industries and particular activities.\textsuperscript{80} Another dimension is added when considering state statutory regulation.

It would be simple enough to write a federal omnibus statute applicable to all commercial actors engaging in any interstate commerce activity. The statute could simply forbid disclosure of consumer information and provide penalties for disclosure on both sides of the transaction. Discussions of omnibus protection raise an interesting question: Why the sectoral approach when all of the statutes essentially do the same thing, prohibit certain disclosures of personal information with law enforcement and course-of-business exceptions? The sectoral approach may be a consequence of federalism. Congress is limited by its enumerated powers, the most important of which for commercial purposes is its Commerce Clause power. States are left to regulate the purely intrastate activities. Also, sectoral regulation may be necessary. Omnibus regulation assumes that privacy concerns are the same for each company and each activity. In reality, the privacy concerns are multidimensional, including unauthorized access, the collection of personal information in centralized databases, and government access to personal information. However, as the European example (explained below) demonstrates, the sectoral approach is neither necessary nor inevitable. Omnibus regulation can work at a multi-national or even a multi-state level.

A final problem to mention is not with statutory protection itself but with the underlying principles that guide the drafting of most federal statutes. Domestically, the Fair Information Practices\textsuperscript{81} were created to help ensure that legislation contains certain minimum protections. At the international level, the Organisation for Economic Co-operation and Development (“OECD”)  

\textsuperscript{80} Solove & Schwartz, \textit{supra} note 2, at 794.
has created its own set of guidelines to help guide privacy legislation in member countries.\textsuperscript{82} The OECD guidelines have influenced legislation in the United States.\textsuperscript{83} However, both the Fair Information Practices and the OECD guidelines are just guidelines. A better solution would be federal legislation that imposed minimum privacy protections.

The European Union’s approach demonstrates how such statutory minimums could be implemented in the United States. The Data Protection Directive\textsuperscript{84} requires member states to create legislation that guarantees minimum privacy protections. The directive also prohibits European Union companies from disclosing data to companies from countries with inadequate protections unless, in the case of US companies, the company complies with Safe Harbor provisions.\textsuperscript{85} Creating legislation similar to the Data Protection Directive would facilitate US trade with Europe. Safe Harbor on a company-by-company basis would be unnecessary.

C. Constitutional Problems

As with the statutory approach, the constitutional approach has resulted in a network of protection, that network being comprised primarily of the 1\textsuperscript{st}, 4\textsuperscript{th} and 14\textsuperscript{th} Amendments. And like the network of statutory protection, information privacy protection at the constitutional level is sectoral. It is sectoral in the sense that the individual is only protected against certain government activities. The 1\textsuperscript{st} Amendment’s only privacy concerns are anonymity and association. The 4\textsuperscript{th} Amendment only covers searches and seizures. The 14\textsuperscript{th} Amendment’s only privacy concerns are due process and liberty. However, there are many government activities that fall outside the pro-

\textsuperscript{82} OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited February 8, 2010).
\textsuperscript{83} Solove & Schwartz, supra note 2, at 998.
\textsuperscript{85} Commission Decision 200/520/EC, 2000 O.J. (L 215) 7 [hereinafter Safe Harbor] (specifying procedures whereby US companies certify they have implemented adequate privacy protections).
tions of these amendments. The amendments do not prevent the government from creating databases of personal information. Once databases are created, the government is generally not prevented from mining the data.86

Constitutional protection is also sectoral in the sense that the existence of a privacy right depends in large part on the actor and on the activity or situation in which the privacy right is claimed. The home is regarded as the most sacred of places.87 At the public sector workplace, the expectation of privacy depends on the employment relation.88 Regarding online activity, at least one court has concluded that there is no privacy in one’s email.89

A sectoral constitutional approach is problematic for the same reasons that a sectoral statutory approach is problematic. It makes constitutional analysis of privacy unnecessarily complex, ironic because the privacy injury is so intuitive. Privacy at the federal level could be protected by one constitutional provision, as it is in some states. The ultimate problem with the sectoral approach in both the statutory and constitutional context is that such an approach leads to multiple, divergent privacy conversations rather than one unified conversation.

D. Market problems

The assertion that the free market can fix just about anything and even address privacy concerns has some merit. The information industry, if you will, is more aware of the threats to information privacy than any other sector of society. Banks, online retailers, and other database owners collect and transmit sensitive information on a daily basis and know best the threats to the information and how best to protect against those threats. The market is able to respond

86 See United States v. Ellison, 462 F.3d 557, 559, 561 (6th Cir. 2006).
quicker than legislatures, enforcement agencies, and the courts. However, the assertion hinges on several assumptions about the relationship between the consumer and the corporate information holder. First, the market approach assumes that corporations care about their customers’ privacy. Secondly, the market approach assumes that customer privacy has some non-de minimis value to both the corporation and the consumer. Finally, it is assumed that the customer and the corporation possess equal bargaining power. None of these assumptions withstands scrutiny.

Imagine a world in which corporations actively and on a regular basis protect the privacy of their consumers from hackers and even the government, absent a warrant. A bookseller would zealously guard its customers’ reading lists against government inquiries. A webhost would fight against improper government requests and fear tactics. Such instances do occur⁹⁰; however, they are the exceptions rather than the rule. The rule is that corporations, especially large corporations, value customer privacy only to the extent that customers feel minimally comfortable with completing business transactions. This attitude is reflected in corporate privacy policies. Most corporate privacy policies are written in broad terms given the corporation great flexibility in how and whether to protect privacy. Many policies contain clauses stating that the policy can be modified at anytime without notice and that information will be given to law enforcement upon valid request.

Privacy policies are generally not enforceable contracts.⁹¹ Even if privacy policies were enforceable, corporations have actively avoided creating legally binding privacy policies. When making a purchase, signing up for a new account, installing new software, or engaging in virtu-

---

ally any other transaction, the customer is required to accept the corporation’s binding terms of use as a condition of receiving the service, using the software, or engaging in any other activity with a corporation. Transactions are rarely, if ever, contingent upon a customer’s acceptance of the corporation’s privacy policy.

On the consumer end, individuals far too often shortchange themselves when valuing their own privacy.\footnote{See Eric Goldman, \textit{The Privacy Hoax}, Forbes, Oct. 14, 2002, http://www.forbes.com/forbes/2002/1014/042.html.} At the University of San Francisco, for example, student representatives are frequently on campus offering “perks” such as free candy or the chance to win a free massage or iPod in exchange for taking a survey or providing one’s email address. Doing either inevitably leads to junk mail and spam. A more common experience is had with discount cards at grocery stores. In exchange for minimal savings on one’s grocery bill, customers are willing to provide their contact information and their family’s eating habits to their corporate grocer.

Related to the valuation problems is bargaining power. If corporations have little regard for an individual’s information privacy, and if individuals chronically undervalue their information privacy, it is highly unlikely that any bargaining over information privacy protection will take place. If bargaining does occur, it cannot be said that the corporation and individual are of equal bargaining power. The corporation knows what information it is collecting, what it does with that information, and is under no obligation to share that information with the individual, absent a statute providing otherwise. Also, as against corporations, customers possess bargaining power collectively, not individually. Most transactions occur on an individual basis, not a collective basis. Hence, there is rarely an opportunity for consumers to exercise their collective bargaining power, if it exists.

There is, however, the Facebook exception. Facebook, and perhaps social networking websites in general, seem to be immune to the valuation and bargaining power problems. Face-
book founder Mark Zuckerberg wrote an open letter to all Facebook users announcing its recent privacy changes. That Zuckerberg cites user demand as inspiration for the changes demonstrates that Facebook users value their privacy and are willing to exercise their collective power to maintain it. Facebook’s privacy changes have also prompted commentary from leading tech websites and blogs, attention of the national press, and a Federal Trade Commission complaint filed by the Electronic Privacy Information Center. Although the particular changes implemented by Facebook are no doubt of great interest, it is important to ask why the media and the public jump every time Facebook sneezes. Why is Facebook subject to so much public attention about its privacy policies while other online entities fly under the radar?

Ironically, public and user responsiveness is facilitated by Facebook itself. Facebook’s architecture allows otherwise dissociated individuals to rally around a common interest are goal. There are several Facebook groups dedicated to expressing their concerns over the social networking giant’s privacy policies. One of the largest such groups, Millions Against Facebook’s Privacy Policies and Layout Redesign, had 2,304,801 members as of February 22, 2010. It is not difficult to imagine this and similar groups organizing a mass exodus if the members become irreconcilably dissatisfied with Facebook’s privacy policies. Without Facebook’s networking tools, such collective action and concern would not be possible.

97 And, more recently, Google Buzz.
Regarding the media, one reason for all the attention may be the Facebook’s rapid growth. Initially launched as a networking site for college students, it now boasts over 400 million members in a mere six years of existence. Several social science articles could be written about Facebook’s evolution and why the public is so sensitive to its privacy policies. From an information privacy perspective, Facebook’s recent experiences may help further explain why the market, at least outside of the online social networking niche, has failed as a regulatory mechanism. If other large companies were as sensitive to privacy as Facebook appears to be, they would likely face similar publicity and backlash over any changes to their privacy policies. Having to spend money on privacy and face public criticism is a scary prospect. However, it is a necessary prospect for Facebook and other companies whose bottom line depends on membership and member activity.

IV. Blame Privacy

Information and Privacy are in a dysfunctional relationship. And none of it is Information’s fault. For starters, Privacy is perpetually beset with identity issues. Legal and social scholars have expended many a word trying to understand Privacy. Among other things, Privacy is the control of who has access to the self, the right to be let alone, and the “right to ‘control of information concerning an individual’s person.’” Ultimately, it may turn out that Privacy cannot be defined succinctly. The definition of Privacy is different for each individual. A YouTube exhibitionist or blogger may reveal certain aspects of his/her life but still chooses what to pub-

---

100 Solove & Schwartz, supra note 2, at 45.
101 Warren & Brandeis, supra note 3, at 206.
lish. A corporate executive may be more open about his sex life than his company’s financial state. This difficulty in pinning down a single definition of Privacy, or a single concept of Privacy, makes its legal protection difficult. The conceptual difficulty manifests itself in the sectoral approach of statutory and constitutional protections, the problems of valuation, and the market’s failure to protect Privacy.

As suggested above, Information Privacy protection may require a sectoral approach because of the different privacy interests at stake. On the consumer’s end, these interests include identity theft, loss of anonymity, possible reprisals for group association, and discrimination based on health and genetic information. That these distinct interests require their own protections is a consequence of the countless conceptions of Privacy. Information does not require such a scattered approach. Information is simply information, a fact or a collection of facts about a given subject. As such, the interests at stake are less wide ranging. Sure, there are different types of information, defined largely in terms of whom or what the information is about. However, the common thread of objective verifiability gives Information a cohesiveness that Privacy cannot achieve, making Information easier to protect.

The valuation problem is also due to the difficulties with conceptualizing Privacy. It can be very difficult to put a price tag on Privacy, both for purposes of determining a remedy for its invasion and for purposes of negotiating transactions. By contrast, it is much easier to put a price tag on Information. For example, the value of having one’s financial information protected against identity theft can be measured by the amount of money in one’s bank account, the value of loans obtained because of accurate credit, and the money saved by corporations in not having to correct the information and not having to comply with breach notification statutes. With data-

103 See supra p. 12.
bases, the value equals increased market share and the profits realized from having access to the database.

The primary reason the market has failed to protect Privacy is because corporations have no direct financial interest in protecting privacy. Take online retailers as an example. If retailers suffered from frequent breaches of customers’ credit card information resulting in identity theft, customers would eventually refuse to shop at the retailer. If identity theft did not exist or if companies could somehow protect customer information without having to implement costly security measures and without having to pay a lawyer to write a privacy policy telling customers how their information is being used, they would probably do so. Corporations do not value consumer privacy for its own sake. Privacy protections are at best prophylactic measures to make consumers feel more comfortable in completing transactions and at worst a corporate investment with little or no return. Information, on the other hand, is a valuable commercial commodity. Customer contact information, market analyses, and purchase histories can make and save companies millions, if not billions, of dollars. Companies can use their information for their own purposes and sell their lists to other companies.

There is a possible exception to the idea that the failures of Information Privacy can be attributed only to Privacy. The newsworthiness element of the public disclosure tort could hinge on the nature of the information, i.e. whether or not the information is newsworthy, and not on the privacy interest at stake. This would be true if courts took a normative approach to newsworthiness. However, the deferential approach, which has been used most often, considers one particular aspect of the information, whether it has been published, equating newsworthiness

\[\text{See supra p. 3.}\]
\[\text{See supra pp. 9-10.}\]
\[\text{See supra p. 9.}\]
with disclosure. This approach places more focus on the privacy interest than the nature of the information.

V. The Case for Information

Information is much more amenable to legal protection than Privacy. Information is easier to conceptualize and define. The interests at stake are more concrete. Information’s value can be more easily assessed. It is much easier to convince corporations to protect Information than to protect Privacy. Information has another feature that makes advocating for its protection attractive: protecting Information protects Privacy.

A. How Protecting Information Protects Privacy

At its core, Privacy is concerned with controlling information of one type or another. Privacy protections, however, are designed to protect and remedy an abstract feeling, a betrayal of some sort. In a sense, protecting Privacy treats the symptoms rather than the underlying cause. Protecting Information, however, prevents and remedies the problem at its source, thereby preventing the privacy injury from ever being realized. Protecting Information opens legislatures’ and industries’ eyes more fully to the privacy interests at stake, and the association of those interests with Information makes them more concrete. Perhaps the best way to illustrate this point is by example.

Consider the EU Data Protection Directive. The Data Protection Directive imposes minimum privacy protections on all member states in order to allow the exchange of personal information, thereby facilitating free trade among member states. A related, but distinct provi-
sion is the Database Directive\(^{109}\), which requires member countries to provide at least sui generis protection for databases. Considering their different historical and legal contexts – the Data Protection Directive being a privacy response to the atrocities of World War II\(^{110}\) and the Database Directive as an intellectual property provision – it is impossible and perhaps inappropriate to discuss the two directives in terms of causation. However, the thought of how these two directives might interact is very interesting. Imagine that a European company has created several databases comprised of consumers’ personal data.\(^{111}\) Assume now that this database meets the minimum requirements for intellectual property protection under the Database Directive.\(^{112}\) Such a database is the intellectual property of its creator but is subject to the minimum privacy protections guaranteed by the Data Protection Directive. In light of the Data Protection Directive’s purpose, enabling the sharing of information, its interaction with the Database Directive produces an intriguing result: the sharing of information without sacrificing privacy or imposing non-recoupable costs on the database owner. The costs of protecting Privacy can be recouped because the database owner can license the information to other companies, provided that privacy rules are followed.

Domestically, the Privacy conversation typically comes about in two ways. As was the case with the Data Protection Directive, a terrible event can prompt the conversation. For example, the Video Privacy Protection Act\(^{113}\) came about as a result of the publication of a Supreme


\(^{111}\) Data Protection Directive, supra note 84, at art. 2(a) (“'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person[.]”).

\(^{112}\) Database Directive, supra note 109, at art. 3 (“[D]atabases which, by reason of the selection or arrangement of their contents, constitute the author’s own intellectual creation shall be protected as such by copyright.”); Database Directive, supra note 109, at art. 7 (“Member States Shall provide for a right of the maker of a database which shows there has been…a substantial investment…to prevent extraction and/or re-utilization…of the contents of that database.”).

Court nominee’s video rental history. The recent Christmas-day bombing attempt re-ignited the debate over the use of full body scanners at airports. The second way the privacy conversation typically comes about is in connection with the recognized need to share personal information. An example of this is HIPAA. Congress passed HIPAA to foster the sharing of health information among health providers and to allow employees to change jobs and insurance without facing gaps in coverage. Because of this recognized need to share information and the sensitive nature of health information, Congress also recognized the need to protect the privacy interests in health information. Although Congress could not agree on specific protections, the Department of Health and Human Services issued health privacy regulations. Privacy protections include patient authorization for non-health related disclosures, accommodation of patient communication preferences, and provision of privacy policies.

The correlation between privacy protections and the recognized need to share information is also present in the Fair Credit Reporting Act (“FCRA”) and the Gramm-Leach-Bliley Act (“GLB Act”). Congress wrote into FCRA its recognition of the need for accurate assessments of creditworthiness and the roles credit reporting agencies play in the financial system. Congress recognized that such information, although sensitive, must be shared under certain circumstances. It is because of this recognized need for sharing information, and not because of pri-

---

114 Solove & Schwartz, supra note 2, at 794.
116 Solove & Schwartz, supra note 2, at 431.
117 Id.
118 Id. at 432.
119 45 C.F.R. § 164.508(a) (2009).
120 45 C.F.R. § 164.522(b) (2009).
121 45 C.F.R. § 164.520 (2009).
vacy’s innate value, that FCRA’s privacy protections\textsuperscript{126} exist. The GLB Act allows the merger of different types of financial institutions, something that was prohibited under prior law.\textsuperscript{127} Such mergers, quite naturally, require the sharing of information. Seeing that financial information is particularly sensitive, especially in light of identity theft, it is entirely appropriate that the GLB Act requires certain privacy safeguards. Again, the need to protect Privacy was recognized in connection with the need to share Information.

As discussed previously, domestic privacy protection is sectoral in nature.\textsuperscript{128} One of two things must occur to foster a comprehensive privacy discussion. Either some very terrible event must occur in such a way as to implicate a broad spectrum of privacy concerns; or the conversation occurs in connection with the recognition and acknowledgment that information is and often must be shared across all industries. Recognizing and legitimizing the need to share information will prompt Congress to be proactive and consider the privacy implications of this need rather than wait for and respond to some large-scale privacy catastrophe.

B. Sui Generis Protection of Information

Privacy concerns are addressed more comprehensively when it is acknowledged that information must be shared. As such, the best way to protect privacy is to allow at least sui generis intellectual property protection\textsuperscript{129} of information and databases. Allowing for at least sui generis protection will acknowledge a practice that is already occurring and allow companies to profit openly. Legitimized sharing of information across all sectors will force the privacy issues to light as real and practical costs of doing business. Advocating for the protection and free flow of in-

\textsuperscript{126} E.g. 15 U.S.C. §§ 1681c-1, 1681c-2.
\textsuperscript{127} Solove & Schwartz, \textit{supra} note 2, at 738.
\textsuperscript{128} See \textit{supra} pp. 5-7, 11-14.
\textsuperscript{129} See \textit{supra} note 112.
formation as a way to protect privacy is admittedly counterintuitive. However, as the examples above demonstrate, this is how the better, more comprehensive privacy protections are created.

Why expand information protection? How would extending intellectual property rights in databases help protect privacy? The motivation behind suggesting at least sui generis protection for databases is two-fold. First, granting protection merely acknowledges and legitimizes a widespread practice, the selling of information for profit. More importantly, acknowledging and legitimizing the practice will likely force the privacy conversation to occur. Suggesting sui generis protection in addition to copyright protection ensures that all databases, even those that do not meet the minimum originality requirements\(^{130}\), receive at least some protection. Such protection should not extend to all bits of information stored with other bits of information. The creator of the database should have to demonstrate that it reaps some non-de minimis value from its possession and use of the database. Also, expanding protection will help facilitate the flow of information and, therefore, facilitate the privacy conversation through all aspects of commerce, supplanting the sectoral conversation that has occurred to date.

The ideal database protection law would combine the Database Directive and Data Protection Directive into omnibus legislation covering all corporate possessors of personal information. In short, databases would be protected by either copyright, if original enough, or sui generis protection, if valuable enough\(^{131}\). In realizing the value from the database, the owner of the database should have to ensure the privacy of its contents – if the database contains personal data\(^{132}\) – by disclosing or selling the information only to domestic companies who are in compli-


\(^{131}\) See supra note 112.

\(^{132}\) See supra note 111.
ance with the new law. Information should not be shared with foreign entities from countries whose laws do not provide adequate protections.

C. As Distinguished from Other Privacy-as-Intellectual-Property Regimes

The idea of importing intellectual property principles to the privacy discussion is not new. Pamela Samuelson suggests trade secrecy and licensing as a model for protecting privacy.133 Paul Schwartz suggests something called “hybrid inalienability.”134 Both suggestions are in response to the idea of granting the individual property rights in her personal information.135 The ideas presented in this article, although having their roots in the privacy-as-intellectual-property discussion, are distinguishable. Rather than advocating for the implementation of a better model for privacy protection, the suggestion of protecting Information is a response to the disparate and sectoral nature of the current privacy conversation. The argument presented here can also be interpreted as advocating the removal of the privacy rhetoric from the conversation, which is admittedly counterintuitive. However, as suggested above and in the conclusion below, discussing Privacy as privacy can create more problems than it solves.

The ideas presented here also differ from those of Samuelson and Schwartz in their aims. The privacy-as-intellectual-property discussion is aimed primarily at the individual, recognizing the individual’s rights in her personal data136 and establishing new default rules for transactions.137 Although noble and ideal, these aims are in contrast to current trends, making the aims all the more difficult to achieve. Mark Zuckerberg’s recent statements provide one interpretation

133 Pamela Samuelson, Privacy as Intellectual Property?, 52 Stan. L. Rev. 1125 (2000). Trade secrecy is often seen as a type of intellectual property protection. Samuelson acknowledges this but presents her idea as rooted in unfair competition. Id. at 1153-55.
135 Samuelson, supra note 133, at 1125; Schwartz, supra note 134, at 2057-58.
136 See Samuelson, supra note 133, at 1134,1151; Schwartz, supra note 134, at 2094.
137 See Samuelson, supra note 133, at 1155-58; Schwartz, supra note 134, at 2100-2101.
of current privacy trends.\textsuperscript{138} Putting more focus on information as a corporate commodity acknowledges that information is shared and sold and will continue to be shared and sold, because of or in spite of the individual’s valuation of her privacy. Most importantly, acknowledging the trade of information will force the privacy conversation to occur in the aggregate rather than in the current splintered fashion.

Julie Cohen has also suggested that something like the Data Protection Directive be imported into US law.\textsuperscript{139} Ms. Cohen advocates the creation of a world in which the individual can learn how to value her privacy, with the goal of reorienting the norms under which society operates, or will soon operate, with respect to privacy.\textsuperscript{140} This would create the conditions under which something like the Data Protection Directive could be implemented.\textsuperscript{141} The ideas presented in this paper are more focused on the corporate end of the information transaction. Viewing things from this perspective and focusing on information maintains current norms while achieving the same privacy protection goals. Adopting something like the Database Directive will create the conditions under which something like the Data Protection Directive can and must exist.

D. Benefits and Drawbacks

A major problem in information gathering is that the data subject often does not know what information is being collected or that information is being collected at all.\textsuperscript{142} A statute fa-

\textsuperscript{138} Sharon Gaudin, \textit{Facebook CEO Zuckerberg Causes Stir Over Privacy}, Computerworld, Jan. 11, 2010, http://www.computerworld.com/s/article/9143859/Facebook_CEO_Zuckerberg_causes_stir_over_privacy?taxonomyId=16 (explaining Zuckerberg’s view that online consumers are getting more and more comfortable sharing their personal information).


\textsuperscript{140} \textit{Id.} at 1424-26.

\textsuperscript{141} \textit{Id.} at 1424.

\textsuperscript{142} \textit{See supra} p. 16.
cilitating the sharing of information would help address the latter problem by bringing information collection practices to light. The statute could also be written to require that all companies tell consumers what types of information they collect. Another approach to solving the problem is to create a nationwide privacy policy, applicable to all entities that collect information from consumers. This privacy policy could lay out the minimum privacy protections all private entities must follow. Each company would be free to implement stricter, binding privacy policies.

At the international level, adopting something similar to the Data Protection Directive would obviate the need for safe harbor. In addition to requiring harmonization of privacy laws, the Data Protection Directive prohibits EU companies from giving information to foreign companies from countries whose privacy laws do not provide adequate protections. The United States negotiated a voluntary safe harbor program with the European Union. This allows US companies to voluntarily comply with EU privacy laws and, therefore, exchange information with EU companies. If the United States were to adopt a comprehensive privacy law similar to the Data Protection Directive, it would join Argentina and Switzerland as countries with whose companies EU companies can freely exchange information.

Granting intellectual property rights in databases could have the unintended consequence of reversing the trend of open consumer access to certain types of information and databases, as marked by the fall of Encarta and the rise of Wikipedia for example. However, it is unlikely that granting such protection will greatly expand the information market and affect consumer access. The point is to acknowledge and legitimize a widespread practice in order to foster the pri-

---

143 Data Protection Directive, supra note 84, at art. 25(4).
144 Safe Harbor, supra note 85.
145 Lothar Determann, Lecture at the University of San Francisco addressing the European Union Data Protection Directive and Safe Harbor (November 10, 2009).
vacy conversation. The suggested changes will only affect corporate treatment of information. On the consumer end, fair use\textsuperscript{147} would still apply. It should apply more liberally where the information is subject to sui generis protection.

Another potential criticism is that protecting Privacy should not have to be done in such a roundabout way. The ideal approach would be to protect Privacy directly. This may turn out to be an aesthetic rather than substantive drawback of the proposed changes. It would certainly be cleaner to address Privacy directly rather than having to catalyze the conversation by protecting Information. However, there is nothing wrong with using A to get to B. The only metric to consider is whether the approach works. The direct approach has not led to the wide-ranging privacy discussion that needs to take place. The privacy discussion seems to yield the best results when it occurs as part of the information discussion.

There are no doubt many more benefits and drawbacks that need to be weighed and discussed. Many drawbacks can be addressed by artful drafting of the statute. One characteristic of many other laws that should be avoided is the creation of exceptions to the law’s coverage. Creating exceptions, whether by industry or by activity, merely allows the problem of sectoral coverage to persist and limits the extent and depth of the privacy conversation. Another aspect that needs to be discussed is how this omnibus statute would interact with federal and state statutes already in place. Ideally, the new statute would not displace any of those statutes. The statute proposed here should set the minimum privacy protections at both the state and federal levels. If an already-existing statute falls below the minimum requirements, it should be amended to meet the new requirements. However, legislatures should be free to pass stricter privacy protections applicable to certain industries, e.g. those that deal with particularly sensitive personal information. Ultimately, however, allowing for more sharing of information and recognizing that infor-

mation is a valuable commodity is the surest way to prompt productive discussion of privacy across all industries.

VI. Conclusion: Why Privacy has such a Bad Rap

Saying Privacy has a bad rap is indeed an overstatement, if not a gross one. Privacy is no doubt an important consideration, especially when discussing the privacy implications of new technology. Perhaps Privacy is simply playing a game it cannot win. To start, Privacy is always a step behind Collection, Use, and Disclosure. Technology evolves so quickly. Commentary and policy discussions quickly follow. However, the law is usually much further behind. It seems like half the battle is figuring out what information is being collected and how it is being used. Many times, one must resort to conjecture and parade-of-horribles arguments that do not always pan out, unless they do\textsuperscript{148} of course.

Although privacy does grab headlines, especially when Facebook is involved or when credit information is stolen, it does not grab headlines in the same way as other topics like discrimination or violent crime. When discrimination, violent crime, or other horrific events occur, there seems to be a collective feeling that something terrible has happened and something must be done. When privacy makes the news, on the other hand, there does not seem to be much collective empathy. If the victim’s embarrassing private life has been disclosed, the average person may say, “Well, had you not been doing that, there would be nothing to disclose.” If the victim’s identity or credit information has been stolen, the average person may check his bank account and credit card statement and say, “That’s unfortunate, but it didn’t happen to me,” or “That’s

\textsuperscript{148} E.g. Olmstead v. United States, 277 U.S. 438, 471-74 (1928) (Brandeis, J., dissenting) (arguing that the Supreme Court’s view of the 4\textsuperscript{th} Amendment should evolve with technology and not apply only to the privacy dangers that existed when the amendment was written and predicting what new technologies may warrant expansion of the 4th Amendment).
why I don’t shop online.” When was the last time a group of concerned citizens organized a widely publicized privacy rally in front of city hall or in Washington, D.C.?

As discussed above, the precise nature of privacy is hard to pin down. It is most intuitively an individual claim of right. It can also be viewed as a public good. Privacy is discussed in terms of identity, decision-making, information, autonomy, technology, etc., etc., etc. Richard Murphy captured this multi-faceted nature by calling privacy a “bit of a chameleon.” It is precisely this chameleon-like nature that makes Privacy difficult to discuss in its own terms.

It is not being suggested that addressing Privacy through Information can immediately and completely address the privacy issues of everyone. Also, it is not being suggested that discussing Privacy in terms of Information will achieve perfect coverage of the privacy harms that may be felt. In fact, this is precisely the point of suggesting a focus on Information. Looking at Privacy through the lens of Information focuses the discussion on those portions of the privacy injuries which are conceptually concrete and legally redressable. The remainder, the nature of which is so difficult to pin down, should be left to society and incorporated into the law as the privacy concept becomes more developed.

---

150 Murphy, supra note 102, at 2381.