BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Privacy 3.0—A Reexamination of the Principle of Proportionality

BY ANDREW B. SERWIN

While there are many disagreements regarding privacy, there is general agreement that current privacy theory does not adequately address growing societal concerns regarding the use and protection of information.[1] The importance of having a comprehensive and cohesive theoretical underpinning for privacy cannot be overstated. The failure to have consensus creates uncertainty for businesses and consumers alike, as it will result in a continuation of the patchwork, and at times inconsistent, approach to regulation that characterizes the laws of today.

A number of law review articles have been written regarding the topic, and significant attention has been focused on the problem, but there is still not consensus on the answer. I raised this question in 2009 in an article entitled ''*Privacy 3.0—The Principle of Proportionality*,'' in which I argued that shifting societal norms required us to rethink privacy.[2] Most recently, on July 21, Federal Trade Commission Commissioner Julie Brill

[1] See, e.g., Erwin Chemerinsky, Rediscovering Brandeis's Right to Privacy, 45 Brandeis L.J. 643 (2007); Neil M. Richards & Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123 (2007). Chris Kelly, The Conversation: Good policy starts with defining what we see as threats, The Sacramento Bee, August 9, 2010, http://www.sacbee.com/2010/08/08/2943056/the-conversation-good-policy-starts.html, last visited Aug. 9, 2010.

Andrew B. Serwin, a partner with Foley & Lardner LLP in San Diego, is the founding chair of the firm's Privacy, Security & Information Management Practice.

[2] ''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.'' Andrew Serwin, PRIVACY 3.0—THE

 ISSN 1538-3423

spoke at the Conference of Western Attorneys General on a panel entitled ''Privacy 3.0,'' in which these issues were raised once again and questions were put forward regarding what the new theory of privacy in the 3.0 world would be given the changes in societal norms, and advances in technology.[3]

Given the changes in society, as well as the enforcement mechanisms that exist today, particularly given the FTC's new focus on its unfairness authority and the well-recognized need to balance regulation and innovation, the overarching principle of privacy today should neither be the right to be let alone, the basis of Privacy 1.0, or a tort-based model that rests on findings of harm, Privacy 2.0, and instead, a different theoretical construct must be created. This is Privacy 3.0—the principle of proportionality. The principle of proportionality balances the sensitivity of data against the benefit to society of collecting or processing data and then categorizes the data into one of four categories based upon this analysis. A key advantage of this model over prior models, as well as proposed models such as ones based upon accountability, is that 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. It focuses regulation on the most sensitive data, provides proportionally appropriate protection, and reduces the potential for overbroad restrictions where there is societal benefit in collecting or processing data.

This article will revisit the principle of proportionality in light of the recent statements from Brill on Privacy 3.0, as well as current state of privacy. It will then identify a path forward for the principle of proportionality.

Privacy 1.0 and 2.0

While the scope of current privacy discussions focuses on Privacy 3.0, modern scholars are not writing on a blank slate. My article discussed two prior theories of privacy, Privacy 1.0 and 2.0, both of which failed to provide a comprehensive, practical, workable theoretical privacy construct. U.S. Supreme Court Justices Samuel Warren and Louis Brandeis identified the theory of Privacy 1.0—the right to be let alone. In light of technological changes, as well as changes in societal values, William Prosser, dean of the College of Law at the University of California Berkeley from 1948 to 1961, put forward a theory based upon common law principles, which became Privacy 2.0.[4] The model advanced by Warren and Brandeis, identified as Privacy 1.0, was the classic formulation of privacy—the right to be let alone—and was driven by the advancement of technology that was seen as radical—the invention of the instant camera.[5] In modern parlance, Warren and Brandeis believed that individuals had the right to notice and choice, including to ''opt-out'' of information collection and processing if they so chose to be ''let alone.''

Dean Prosser, relying upon the common law, creating four distinct torts: intrusion upon seclusion; appropriation of name or likeness; publicity given to private life; and publicity placing a person in false light, believing this approach would bring order to the chaos. These torts became the basis of the Restatement Torts formulation of privacy, as well as the basis of Privacy 2.0.[6] The inherent problem with a tort-based approach was foreshadowed by Warren and Brandeis in their rejection of property law as a basis for privacy, which is the element of harm inherent in any tort-based model.[7]

In the end, the requirement than an individual show he or she was harmed by a privacy violation doomed Privacy 2.0 to failure, and the key stakeholders in privacy agree that both prior and current theories of privacy do not function properly. In rejecting ''the right to be let alone,'' and Prosser's harm-based model, I argued that Privacy 3.0 should be governed by the principle of proportionality. This was particularly important given the need to balance regulation and innovation; as well

---

PRINCIPLE OF PROPORTIONALITY, 42 U. Mich. J.L. Reform 869 (2009).

[3] Brill stated: ''So the debate underway now in Washington is what can we do to make a better model for dealing with privacy in this 3.0 realm. And there's been a lot of discussion at the Federal Trade Commission about this, a lot of discussion in DC and a lot of discussion going on in Silicon Valley. I don't think there is any consensus about the precise shape that regulation ought to take in this 3.0 realm.'' A video recording of the presentation can be found at http://blogs.berkeley.edu/2010/07/21/commissioner-brill-and-privacy-3-0-at-the-cwag- privacy-panel-2/, last visited Aug. 10, 2010.

[4] ''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, 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.'' Serwin, supra note 2, at 869.

[5] ''While Warren and Brandeis are often credited with creating the right of privacy, they certainly did not do so. What they did do, however, is provide the theoretical construct that helped shape the parameters of privacy protection in the United States. Ultimately, while serving on the Supreme Court, 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. 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.'' Serwin, supra note 2, at 870-871.

[6] Id.

[7] The Prosser/Restatement model is based in tort theory. Inherently, this limits its usefulness in addressing the privacy issues of today. Ironically, 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.' '' Serwin, supra note 3, at 884. This is the same failing of tort theory providing the basis of Privacy 2.0.

  PVLR ISSN 1538-3423

as the fact that overbroad restrictions on information can damage consumers as well as society.[8]

Commissioner Brill's Recent Comments on Privacy 3.0

Brill, in recent comments on Privacy 3.0, discussed the failings of the prior iterations of privacy. Under Brill's model, Privacy 1.0 represented the government views of privacy from the mid-1990's. Brill summarized Privacy 1.0 as follows:

> So, let's go back and think about what Privacy 1.0 was. Privacy 1.0 from my perspective was the notice and choice model, or what we used to call Fair Information Principles and it's something that everyone is familiar. In fact General McKenna [Washington Attorney General Rob McKenna (R)] was touching on it. It basically started in the mid-1990s and the FTC and the states were looking at privacy issues through this lens. They were looking for notice, choice, access and security with respect to information. And they evaluated, we all evaluated, privacy policies on the web that way, we looked at practices of companies that way, we looked at various self-regulatory regimes through that lens.[9]

Brill then defined Privacy 2.0 as follows:

> But shortly after the Gramm-Leach-Bliley Act (the ''GLB'') was enacted the Federal Trade Commission, as some of you may know, switched gears, and moved from Privacy 1.0 to Privacy 2.0. So it moved from the concept of fair information principles to a harm model. And the harm-model was first launched by then Chairman Tim Murris, but it has since has been picked up by many, many folks including in the states. The harm model is one that focuses on harmful practices that present risks of physical security or economic injury. So the things that the Federal Trade Commission started focusing on and frankly the states started focusing on were data security, data breaches, which are a subset of data security, identity theft, children's on-line privacy, and things like spam, spyware and telemarketing through the national do-not-call list. So just focusing on the first two, data security and data breaches, what a lot of the regulators did during this timeframe was focus on how to enhance tools that the federal government and the states had with respect to data security and data breaches.[10]

In summarizing the current state of Privacy 2.0, Brill stated:

> So what about the harm-model? The model that looks at is there some kind of tangible harm to consumers either economic or perhaps psychological or whatever? Well it really doesn't address the exposure of sensitive information the kind of medical conditions we were talking about. It doesn't also really address what's happening perhaps with children through behavioral advertising. Also more fundamentally the harm-model is a reactive model, what it says is once we determine that there has been harm, we will try to recompense those who have been harmed. It doesn't try to take a forward-looking approach where we say: ''How can we set up an architecture or system that tries to avoid as much of the harm as possible?'' So as opposed to being proactive the harm-based approach is really a reactive approach.[11]

If Privacy 2.0 is not the answer, it necessarily follows that Privacy 3.0 is. However, as noted earlier, Brill stated that there was not consensus on what Privacy 3.0 should be. While consensus does not yet exist, I believe that adopting the principle of proportionality as the theoretical construct is the appropriate answer.

Defining Privacy 3.0

In *Privacy 3.0*, I argued that 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 should be built upon one principle—the principle of proportionality.[12] While as a construct, 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 would vary according to the sensitivity of the information, as would the methods that can be used to collect, process and use information. This permits the implementation of this theoretical construct in a way that will not stifle innovation and that will also permit sufficient flexibility to address new forms of information as they become more relevant to society.[13]

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 (e.g., predispositions,

[8] 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.'' Serwin, supra note 2, at 875-876.

[9] Comments by Commissioner Julie Brill, July 21, 2010, Conference of Western Attorneys General, http://blogs.berkeley.edu/2010/07/21/commissioner-brill-and-privacy-3-0-at-the-cwag-privacy-panel-2

[10] Comments by Commissioner Julie Brill, July 21, 2010, Conference of Western Attorneys General, http://blogs.berkeley.edu/2010/07/21/commissioner-brill-and-privacy-3-0-at-the-cwag-privacy-panel-2/, last visited Aug. 10, 2010.

[11] Comments by Commissioner Julie Brill, July 21, 2010, Conference of Western Attorneys General, http://blogs.berkeley.edu/2010/07/21/commissioner-brill-and-privacy-3-0-at-the-cwag-privacy-panel-2/, last visited Aug. 10, 2010.

[12] Serwin, supra note 2, at 875 .

[13] Serwin, supra note 2, at 900-901.

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. Perhaps one of the most important factors—the social utility of sharing 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 often subject to reduced protection. 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 another 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.

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 flow from the tier within which the category of information falls. Thus, there are common elements regarding each tier that include:

- whether information can be gathered without notice or consent;
- whether consent must be opt-in or opt-out;
- the effect of consent;
- the types of processing that can be conducted;
- if information can be gathered under false pretenses;
- whether there time restrictions on the retention of the data;
- data security requirements;
- data destruction requirements;
- the steps 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.[14]

The following is a summary of the tiers. Given the scope of this article, a more detailed discussion of the tiers, as well as examples of where these classifications are already implicitly recognized, is not included.[15]

Tier I—highly sensitive information—would be subject to strong limitations on the collection and processing of information. Examples 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), and highly proprietary or confidential business information. While most collection and processing would be done only with notice and consent, there are examples where even the government can collect information without consent. This includes genetic information in certain circumstances, as well as mandatory disclosures of certain communicable diseases and medical information in connection with electronic health records. If consent by the consumer is given, additional collection and processing can be conducted of Tier I data.[16] This type of data would typically be subject to high levels of data security and violations of laws governing Tier I data could give rise to both civil and criminal sanctions.

Tier II—sensitive information—includes quite sensitive information, but it is not information that rises to the same level of sensitivity as Tier I information. Examples of Tier II information include the content of wire or electronic communications (if gathered precisely at the time of the communication), certain forms of health information, 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 under its Foreign Intelligence Surveillance Act and USA PATRIOT Act 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 no longer needed 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 could not be proven.

Tier III—slightly sensitive information—is personally identifiable information of a lower privacy profile than the information in Tiers I and II. To the extent the information would be sensitive, Tier III would be made up 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 internet protocol (''IP'') addresses of websites visited, as well as to/from addresses for email, have also been held, at least by the U.S. Court of Appeals for the Ninth

[14] Serwin, supra note 2, 902.

[15] For a more detailed discussion of the data classification possibilities, as well as examples of where existing laws follow this pattern and examples of laws that have created confusion because they fail to account for sensitivity. *See* Serwin, supra note 2, 902-930.

[16] As an example, consider the Health Insurance Portability and Accountability Act medical marketing restrictions that require a covered entity to obtain the authorization of the consumer to further process already collected information.

  PVLR ISSN 1538-3423

Circuit, not to be private, based upon a pen register analogy.[17] Consequently, these records would fall in Tier III. 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 Tiers 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.

Tier IV—non-sensitive information—is comprised of information that may identify a person, but is not truly private. Examples of Tier IV information would include a 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.

A Path Forward

The principle of proportionality offers a viable theoretical construct for Privacy 3.0. Classifying data in this way will permit consistency in the application of laws, as well as permit companies to adopt consistent practices when new forms of data become relevant, even if the data is not yet covered by existing laws. However, work needs to be done for the principle of proportionality to provide a path forward.

Studies must be conducted in which individuals are asked to assess the sensitivity of categories of data. Through this analysis we will have part of the picture regarding how information should be protected, this is only half of the equation. Studies must also be done of the uses of information by government and businesses in order to assess, for a lack of a better term, the value of the categories of data. It is only through learning how people truly assess the sensitivity of certain types of information, as well as the value that exists when the data is processed, that we can understand how to proportionally regulate data. In cases where there is little sensitivity and high value, little to no regulation should exist. Conversely, where there is high sensitivity and high value, regulations must be strict, but balanced against truly legitimate and appropriate government or business needs. An example of this scenario is one noted earlier in this article—an individual's health information as it is placed in electronic health records. While it is hard to imagine a more sensitive type of information, government has not given us a choice regarding the collection or processing of this data in electronic and interoperable form, based upon the government's legitimate interest in reducing costs and poor outcomes based upon a lack of accurate information in patient's records.

Shifting from a harm-based approach to one based upon proportionality will permit regulators and business alike to try and align expectations regarding the regulation and use of information, particularly once studies are done regarding the sensitivity and value of data. These issues will be the subject of future studies and articles that will offer further suggestions on how to chart the correct course to Privacy 3.0 that will permit proportional regulation to be adopted. While over time the types of information might move within the tiers, the structure, and the general restrictions tied to each tier, will not change. This structure 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.

Answering the question of what Privacy 3.0 will be is an important question that must be answered quickly so we can adopt consistent and appropriate regulation of information practices and because, as I noted in 2009, ''Facebook and Flickr await.''[18]

---

[17] *United States v. Forrester*, 495 F.3d 1041, 1048-49 (9th Cir. 2007) (6 PVLR 1117, 7/16/07).

[18] Serwin, supra note 2, 930.