A PRACTICING PRIVACY LAWYER'S PERSPECTIVE ON USE ANALYSIS AS A WAY TO MEASURE AND MITIGATE HARM

BY CHRISTOPHER WOLF*

INTRODUCTION

Many businesses today understand that privacy is more than just a legal obligation. It is an obligation that goes to the fundamental issues of consumer trust and reputation. If businesses use legally collected data in ways that violate privacy expectations, they may lose consumer trust; they also could suffer a loss of public reputation, be subject to media scrutiny, or be subject to increased regulatory and congressional oversight. Additionally, because privacy law is constantly adapting to changes in technology, the traditional application of privacy rules may become strained with each new innovative leap in the collection or use of data. Sophisticated companies understand that to meet consumer expectations of privacy, they must look beyond traditional legal requirements and follow a kind of corporate Hippocratic Oath to do no privacy harm.

Consequently, privacy lawyers increasingly are called upon to help

* Christopher Wolf is director of the global Privacy and Information Management practice at Hogan Lovells US LLP, and is the founder and co-chair of the Future of Privacy Forum. Special thanks to Hogan Lovells colleagues Jared Bomberg and James Denvil for their assistance in the preparation of this essay.

their clients respect consumers' privacy well beyond just meeting basic legal requirements. This essay discusses those tasks facing a privacy counsel. It explains the basic legal framework to remedy privacy harm, shows why privacy lawyers should be warry of focusing excessively on this basic framework, and proposes a way for privacy counsel to advise clients on a broader set of privacy harms that reflects privacy risks companies need to consider.

Underpinning this discussion is the question of privacy harm. If privacy harms were appropriately captured by the current law, privacy lawyers could look to existing rules to provide checklist answers to clients. They could reference a statute, regulation, interpretative document, enforcement action, or case and find guidance and create a compliance strategy. But harms are not sufficiently captured through the existing framework, and privacy lawyers are therefore tasked with providing advice that goes beyond basic legal requirements.

COUNSELING BUSINESSES ON COMPLIANCE WITH THE LAW AND AVOIDANCE OF BROADER PRIVACY HARMS

The Basic Legal Framework for Privacy Practitioners

From a practitioner's point of view, the primary mechanism by which privacy harm is captured—and liability imposed—is through privacy misstatements. If an organization fails to live up to the privacy promises it has made in privacy policies, marketing materials, or other public statements, this is a privacy violation that the law recognizes.[1] Similarly, an organization that collects, uses, or discloses information about consumers in a way that those consumers would not ordinarily expect without providing sufficient notice is another form of a legally recognized privacy violation.[2] Put more simply, to a large degree privacy law has become the law of broken promises and the law of inadequately

1. *See* Eli Lilly & Co., 133 F.T.C. 20, at *2 (2002), *available at* http://www.ftc.gov/os/caselist/0123214/0123214.shtm (alleging that Eli Lilly committed a deceptive trade practice when it sent an email to consumers who signed up for an online service that included all email addresses within the "To:" field, thereby unintentionally disclosing email addresses in violation of its representation that "Eli Lilly and Company respects the privacy of visitors to its Web sites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource.").

2. *See* Sears Holding Mgmt. Corp., FTC File No. 082 3099 (Complaint Sep. 6, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/index.shtm (alleging that Sears committed a deceptive trade practice when it provided a downloadable software application to consumers that it said would track their "online browsing" without disclosing that the software would collect sensitive information from the consumers' web activities, such as the contents of shopping carts, online bank statements, drug prescription records, video rental records, library borrowing histories, and information from web-based emails).

disclosed information practices.

Privacy liability also arises when plaintiffs allege violations of statutes that set privacy and security rules. In the areas of health data, financial data, and children's data, for instance, existing statutory rules create liability for specific entities and activities covered by these acts. Additionally, plaintiffs have begun bringing privacy lawsuits based on supposed violations of federal statutes that protect electronic data generally, such as the Electronic Communications Privacy Act, even when the statute sometimes has a tenuous connection to the underlying privacy harm.[3] Courts have allowed these cases to proceed based solely on alleged violations of these statutes even when no harm has been shown.[4]

But, does this legal framework—which imposes liability due to inadequate privacy representations and violations of federal statutes—too often inappropriately punish practices that only minimally affect privacy? And, does it capture all privacy harm that needs to be captured? For many businesses and consumers, the answers are yes and no, respectively. The reality is that if avoidance of harm is the goal, too much time is spent parsing privacy promises and debating technical hooks to statutes.

The Risks of Counseling Based On the Basic Legal Framework

The current legal framework raises important questions for privacy lawyers to consider when advising clients.

On the one hand, the current framework may be over-inclusive of privacy harm because a technical violation of a written privacy policy

3. *See, e.g.*, *In re* Hulu Privacy Litig., No. C 11–03764 LB, 2012 WL 2119193 (N.D. Cal. 2013); Gaos v. Google, Inc., No. 5:10–CV–4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (holding that the federal Stored Communications Act "provides a right to judicial relief based only on a violation of the statute without additional injury"); *In re* Facebook Privacy Litig., 791 F.Supp.2d 705 (N.D. Cal. 2011) (finding standing where plaintiffs alleged a violation of ECPA); Zynga Privacy Litig., No. C 10–04680, 2011 WL 7479170 (N.D. Cal. June 15, 2011) (holding that a violation of statutory rights under the Stored Communications Act provides Article III injury); Cousineau v. Microsoft, No. C11-1438-JCC, 2012 WL 10182645 (W.D. Wash. June 22, 2012) (denying motion to dismiss for lack of Article III standing where plaintiff alleged an SCA violation). *But see* Van Alstyne v. Elec. Scriptorium, 560 F.3d 199 (4th Cir. 2009) (ruling that a plaintiff must prove actual damages to recover a statutory award under the Stored Communications Act); Sterk v. Best Buy Stores, No. 11 C 1894, 2012 WL 5197901 (N.D. Ill. Oct. 17, 2012) (finding claim for violation of Video Privacy Protection Act based on alleged disclosure of plaintiff's movie purchase history insufficient to confer Article III standing).

4. Harris v. comScore, Inc., 292 F.R.D. 579 (N.D. Ill. 2013) (Plaintiffs claimed that the defendant, an online data research company, unlawfully collected data about their activities on the internet and sold that data to third parties in violation a number of federal statutes that impacted electronic data. The court certified a putative privacy class in this case, notwithstanding uncertainty about the existence and amount of plaintiffs' actual damages.).

does not necessarily equal actual privacy harm. Too many attempted class actions seize on technical violations where there has been no harm of the sort most consumers care about. Similarly, plaintiffs are latching on to laws with statutory damages in the hope that proving a technical violation of the law will remedy alleged privacy harm. The recent class action against Google over its email service, Gmail, is a prime example.[5] The lawsuit alleges that Gmail is violating federal and state statutory law by having an automated processor scan emails sent from non-Gmail accounts even though all Gmail account holders have consented to this activity.

On the other hand, a privacy regime focused on privacy policies and statutory violations may be under-inclusive because it misses many types of harm. For instance, intangible harms, like embarrassment and social stigma, are not covered. There is a wide range of potential harm stemming from the use of information that is true but harmful to someone's reputation.

One example is where a teenage boy or girl uses the internet on a family computer to look up information about sexual identity, with the result that revealing information (like a targeted ad) is pushed to that computer when the parent is using it, essentially "outing" the teenager. Multiple harms can flow from such a scenario, from emotional stress to being disavowed when the parent discovers their child is gay. Unwanted inadvertent disclosure or suggestion of intimate information can result in emotional harm that is not subject to legal remedy because it is not covered in our privacy harm framework, which is based on broken promises or statutory injuries. To fully inventory intangible harms, from the "outing" example to the much-mentioned examples of people feeling like they are being watched, is not easy. But the fact that lawmakers or regulators may not be able to capture all of these harms does not mean that businesses should not undertake on their own to avoid intangible harm while continuing to innovate.

Finally, privacy lawyers have to be cognizant that the underlying legal regime may fail both businesses and consumers when privacy policies provide for the broadest possible uses of data, use complex or vague terms that consumers do not fully grasp, or are excessively lengthy. In egregious cases, some privacy policies use broad and vague terms that can mean an individual's consent surrenders all of that person's data for nearly any purpose.[6] For instance, the company

5. *In re* Google Inc. Gmail Litigation, No. 13–MD–02430–LHK, 2013 WL 5366963 (N.D. Cal Sep. 25, 2013).

6. Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 649 (2014) ("[P]rivacy policy promises have not progressed toward being more specific. If anything, they have become more vague as lawyers

Echometrix's former privacy policy stated, "[Sentry] uses information for the following general purposes: to customize the advertising and content you see . . . improve our services . . . conduct research, and provide anonymous reporting for internal and external clients."[7] While these terms may be accurate, they do not provide clarity to consumers looking to make an informed choice.

Similarly, the sheer length of privacy policies can make it difficult for consumers to understand what they are consenting to. A consumer advocacy group reported in 2012 that when PayPal's privacy notice is added to its other terms of use, the total word count is 36,275 words, longer than *Hamlet*, which totaled 30,066 words.[8] Aleecia McDonald and Lorrie Cranor calculated that reading the privacy policies of just the most popular websites would take 244 hours, more than 30 full working days each year.[9] Privacy lawyers should be mindful of the fact that the more complex or vague the representation, the more likely it is that information practices will not be well understood by consumers. This can lead to both legal liability and public relations risks.

Thus, many businesses that want to do the right thing are lost when it comes to implementing a comprehensive set of privacy practices that both meet consumer expectations and avoid stifling innovation. The law only provides partial answers about privacy harms. Businesses also know that with the ambiguity in definitions in consumer protection law, and with lawmakers focused as never before on privacy, they have to avoid using data in ways that might cause regulatory enforcement or spur new, over-reaching public or enforcement backlash. Therefore, when businesses set out to evaluate what constitutes harm that they should avoid inflicting on customers, statutes and precedent are only a starting point.

Privacy Interests Are Served By Focusing On the Misuse of Data

Privacy lawyers looking to counsel clients beyond privacy representations and potential statutory liability on a broader set of harms clearly need to think beyond the basic framework. A more accurate

have attempted to avoid language that pins companies down on specifics.").

7. FTC v. Echometrix, FTC File No. 102 3006 (Complaint Nov. 30, 2010), *available at* http://ftc.gov/os/caselist/1023006/101130echometrixcmpt.pdf.

8. Rich Perris, *Online T&Cs longer than Shakespeare plays – who reads them?,* WHICH? (Mar. 23, 2012), http://conversation.which.co.uk/technology/length-of-website-terms-and-conditions; FRED H. CATE & VIKTOR MAYER-SCHÖNBERGER, CENTER FOR INFORMATION POLICY RESEARCH, DATA USE AND IMPACT GLOBAL WORKSHOP (2013), *available at* http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf.

9. Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. OF LAW & POL. 543 (2008); FRED H. CATE, ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY (2013).

measure of harm, and possibly a better privacy framework, is one that would focus on counseling against the "misuse" of data.

Misuse, under this new privacy framework, would include both tangible and intangible privacy harms. Identity theft, wrongful disclosure of information, blackmail, and physical harm are all examples of tangible harms that could stem from a privacy violation.[10] Similarly, spam, junk mail, and other unwanted solicitations also can be viewed as a tangible harm since they cause consumers to waste time and money protecting against such activities.[11] Intangible harm includes reputational and emotional harm and the chilling effects of surveillance. Additionally, breaking a privacy promise, which could lead to either tangible or intangible privacy harm, would be considered a misuse of data.

One way for a privacy counsel to explain misuse to clients is to advise them to examine the context under which individuals surrendered their data and then compare it to the context in which they are considering using it. Data collected in one context, for example through cookie-based online tracking, might be inappropriate to use in a different context, for example, in determining eligibility for a job.[12] Context is a strong indicator of an individual's expectations; it also provides insight into how individuals think about their personal data. Context can be broken down by examining: 1) the type of data being volunteered; 2) the service into which it is being transferred; 3) how the information is normally used; 4) the type of device on which the transaction is being made; and 5) whether the data was collected passively or actively.

Additionally, under a misuse framework, privacy lawyers should counsel their clients that certain data sets need heightened protections. For instance, sensitive personally identifiable data and big data sets may require their own safeguards. Retention limitations, de-identification, and enhanced data security are tools to protect such data and avoid misuse.

Over time, our conception of use and misuse will grow to better reflect actual privacy harms. This privacy framework will not be caught on technicalities and will not be a pretense for alleging statutory violations. The privacy community, which is expanding rapidly, will participate in airing and vetting appropriate use and in defining such use. For instance, thought leaders such as Fred Cate and Viktor Mayer-Schönberger, and practitioners such as Marc Groman of the Network Advertising Imitative, recently championed movement towards a "use" framework.[13] Companies in doubt can convene outside consultants,

10. Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. ON TECH. & INTELL. PROP. 321, 339 (2013).

11. *Id.*

12. *See* CATE & MAYER-SCHÖNBERGER, *supra* note 8.

13. *See* CATE ET AL., *supra* note 9; Marc Groman, *Thoughts on an 'Updated Privacy*

consumer groups, and even visit regulators like the Federal Trade Commission for input and blessing. Some have suggested the creation of groups akin to Independent Review Boards (often used for health data and government access to data) to review and comment on misuses. Each of these steps could help entrench a legal framework that more accurately captures and measures privacy harm. Additionally, privacy lawyers would benefit from such discussions as they would yield a better roadmap for lawyers to point to as they counsel clients.

CONCLUSION

Fundamentally, privacy lawyers have an important role to play in counseling on existing law, but also in understanding the winds of change and where gaps in current law exist. It is the responsibility of privacy lawyers to help fill in those gaps for their clients and help position them for the future. In the case of privacy law, businesses expect lawyers to anticipate all types of harms and to help them meet consumers' expectations even beyond the basic legal requirements. Consequently, there is a need and opportunity for the privacy profession to develop common understandings about what constitutes privacy harms and how to avoid them. A framework based on the proper use of data would be one way to do so and may be a more accurate gauge of harm. As the ranks of privacy professionals grows, so too do the opportunities for consideration and collaboration on the appropriate use of data. Together, we can do a better job of measuring and protecting against privacy harms, and I look forward to that ongoing process.

Paradigm for the Internet of Things', NETWORK ADVERTISING INITIATIVE (Jan. 23, 2014), http://www.networkadvertising.org/blog/thoughts-updated-privacy-paradigm-internet-of-things.