Maine Law Review

Volume 66
Number 2 *Symposium: Who's Governing Privacy? Regulation and Protection in a Digital Era*

Article 2

June 2014

Foreword

Peter J. Guffin
University of Maine School of Law

Kyle J. Glover

Sara M. Benjamin

FOREWORD

Peter J. Guffin, Esq., Kyle J. Glover, Esq., and Sara M. Benjamin, Esq.[*]

"It seems . . . that the advance of civilization is nothing but an exercise in the limiting of privacy."

—Isaac Asimov, *Foundation's Edge* (1982)

In their seminal 1890 article, *The Right to Privacy*, Samuel Warren and Louis Brandeis observed:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the housetops."[1]

What is remarkable about this comment is that it could be applied with equal force to today's world. Although the technologies are different—instant photographs and sensational tabloids have been replaced by Google Glass and tracking technologies—the impulse "to be let alone" and the fear that "what is whispered in the closet shall be proclaimed from the housetops" remains relevant to today's privacy concerns.[2]

In fact, perhaps the only constant in the modern era has been an almost breathless sense of change, a sense that new and unpredictable developments are just around the corner, and that today's way of dealing with things may not be up to tomorrow's task. Nowhere is this more evident than in the area of information and privacy, where technological changes have facilitated an exponential increase in our ability to communicate and to know. According to Eric Schmidt, the former CEO of Google, approximately five exabytes of information were created between the dawn of civilization and the year 2003.[3] Today, the same amount of information is created in less than two days.[4] Most of this data, according to

---

* Peter J. Guffin is Chair of Pierce Atwood LLP's Intellectual Property and Technology Practice Group and heads the firm's Privacy & Data Security Practice. Kyle J. Glover and Sara M. Benjamin are members of Pierce Atwood LLP's Intellectual Property and Technology Practice Group and Privacy & Data Security Practice. The Authors would like to thank the Maine Law Review, and in particular, Editor-In-Chief Amy Olfene and Symposium Editor Sara Murphy, for their tremendous efforts putting together the Symposium, *Who's Governing Privacy? Regulation and Protection in a Digital Era.*

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citation omitted).

2. Also interesting, of course, is that the instant photograph, which was the source of such consternation and concern in 1890, is now virtually ubiquitous and rarely remarkable.

3. MG Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003*, TECHCRUNCH (Aug. 4, 2010), http://techcrunch.com/2010/08/04/schmidt-data. This quote has been criticized, but the disagreement has been on the numbers used, not the fact that the pace of data generation is increasing rapidly.

4. *Id.*

Schmidt, is user generated—Facebook pages, text messages, blogs, etc.[5] As our social relations are increasingly recorded and collected, the risk that information that we think we are "whispering in the closet" is in fact being "proclaimed from the rooftops" have only increased.

Policymakers and thinkers grappling with this issue face a conundrum. The pace of change has, in many ways, outstripped our ability to grasp and deal with it. How does Alan Westin's definition of privacy as the ability "'to control, edit, manage, and delete information' about themselves, and to 'decide when, how, and to what extent information is communicated to others'"[6] fare when Big Data is generating information about us that we do not even know ourselves? How can lawmakers legislate solutions to the problem when laws are outdated by the time they take effect?[7] It's not even clear that our culture and expectations have kept up, and we therefore face powerful antecedent questions: What do we even want as a society? How do we collectively go about answering that question?

In this context, the Maine Law Review's Symposium, *Who's Governing Privacy? Regulation and Protection in a Digital Era,* could not have been more timely. The papers presented during the Symposium (and collected here for your consideration) are an important contribution to the discussion.

In a Big Data world, vast amounts of information are gathered for uses often unforeseeable at the time of collection. If we are to capitalize on Big Data, we may need to rethink our privacy policy objectives, many of which are rooted in the Fair Information Practice Principles of notice, choice, access, security and enforcement,[8] and may no longer be practicable. In an effort to reshape our privacy policies, Dennis Hirsch, in his piece, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, suggests we draw from the valuable lessons of environmental law. Analogizing the harms caused by Big Data to those caused by the use of fossil fuels, Hirsch posits that data breaches are like oil spills and that the accumulation of data concentrates the glare of public scrutiny in much the same way the accumulation of greenhouse gases traps the sun's heat. Based on this understanding of the similarities between environmental and privacy harms, Hirsch argues privacy laws should be modeled after environmental laws, which have successfully reduced environmental damage by, among other things, expanding tort liability and incentivizing risk-reducing technologies.

Bryce Clayton Newell furthers this discussion by highlighting the complexity of privacy policies as they pertain to the use of Big Data by government agencies and local law enforcement. In his article, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition System, Information Privacy, and Access to Government Information*, Newell illustrates the benefits

---

5. *Id*.

6. L. Gordon Crovitz, *Privacy Isn't Everything on the Web: Online Social Norms Eventually Catch Up with What the Technology is Capable Of,* WALL ST. J., May 24, 2010 12:01 AM, http://online.wsj.com/news/articles/SB10001424052748704546304575260470054326304.

7. *See* 18 U.S.C. §§ 2510-2522 (2012 & Supp. 2013); Council Directive 95/46, 1995 O.J. (L 281) (EC).

8. *See generally* FED. TRADE COMM'N., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (May 2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

derived from government use of Big Data, but also the privacy implications of making such information available through freedom of information laws. To drive home this tension, Newell looks at automated license plate recognition surveillance techniques currently being used by law enforcement agencies throughout the country, as well as the freedom of information laws that make much of this information available to members of the general public. The privacy harms created by collecting and making such information publicly available, he argues, must be weighed against the benefits of better enforcement from such surveillance and of public oversight derived from such freedom of information laws.

Recognizing the privacy problems new technologies present, it is imperative that we examine possible solutions including multistakeholder processes, legislation, education, and development of new technologies. Omer Tene and J. Trevor Hughes, in their piece, *The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study*, look at multistakeholder policymaking in the case of developing a Do Not Track ("DNT") standard in web browsing. Based on their case study, Tene and Hughes conclude that stakeholder consensus is difficult to achieve in the absence of robust process design and a legitimate threat of government action if consensus is not achieved. This is particularly true where, as in the case of DNT, there are a large number of stakeholders with strongly opposed interests.

Adam Thierer, by comparison, points out the stifling effect legislation can have on technological innovation and instead argues for a bottom-up educational solution in his article, *Privacy Law's Precautionary Principle Problem*. Thierer asserts privacy legislative efforts driven by the precautionary principle—that new innovations should be curbed until proven safe—err too much on the side of safety, thus preventing valuable innovative efforts. Drawing on the history of online child protection efforts, Thierer argues education is a better solution.

Cloud computing further complicates the debate. It raises concerns about transnational surveillance and the proper technical and legal restrictions placed on third-party access to cloud-based storage. Joris van Hoboken and Ira Rubinstein, in their article, *Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, discuss the cloud industry's technological responses to transnational surveillance and suggest that technological solutions can help shape lawful access. Such technological responses, they argue, will increasingly be used to 'regulate' government data access in order to enhance privacy and information security protections. However, questions remain as to whether governments may be able to legally compel providers to break their security models, undermining these technological solutions.

Although these papers do not answer all of our questions, they provide powerful insight from leading scholars and bring us closer to addressing one of the biggest challenges of our times. One thing, at least, has not changed since 1890: the work of scholars and the dialogue resulting from their work remain crucial aspects of our attempt to grapple with these questions. By reading these articles and grappling yourself with the ideas presented therein, we invite you to participate in the conversation that Warren and Brandeis began.