MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 40 | Issue 2 Article 2

2014

Foreword

Megan J. Hertzler

FOREWORD

Megan J. Hertzler†

As I am typing the foreword on my laptop, effortlessly editing it without spilling ink from a fountain pen or filling a trash bin with crumpled paper, I take a moment to absorb how technology has transformed the world over the past century. Evolving at an ever-faster pace, technology has both given us superpowers and rendered us vulnerable by making our resulting dependence an Achilles' heel. The tension between functionality and dependency affects each one of us. For example, when on a road trip I do not bring a map, but rather I trust my smartphone to direct me to my destination. But when the reception for my smartphone—and the technology—is lost, so am I.

In my professional life, focused on information governance in the utility industry, I am following with cautious enthusiasm the development of one of the most promising technologies on the horizon, the Smart Grid.[1] Similar to other recent advances in technology, the Smart Grid is a vision of a future where billions of digital devices and machines of all kinds will communicate with each other to automate tasks and, we hope, improve our lives.[2]

† Director of Information Governance at Xcel Energy, a combination electricity and natural gas utility company operating in eight midwestern states (www.xcelenergy.com). The Information Governance department at Xcel Energy is responsible for policy, strategy, and compliance for protecting Xcel Energy's high-risk and high-value data. Ms. Hertzler is also a 1997 graduate of William Mitchell College of Law.

1. The "Smart Grid" generally refers to advanced technology for the delivery of electricity that utilizes computer-based remote control and automation. An important aspect of this technology is the use of two-way communication technology and computer processing. For further definition of the "Smart Grid," see *Smart Grid*, U.S. DEPT. ENERGY, http://energy.gov/oe/technology-development/smart-grid (last visited Dec. 21, 2013), and SMART GRID LIBR., http://www.smartgridlibrary.com (last visited Dec. 21, 2013).

2. Steve Lohr, *A Messenger for the Internet of Things*, N.Y. TIMES (Apr. 25, 2013), 2013 WLNR 10079927; *see* Dave Evans, *Thanks to IoE, the Next Decade Looks*

Some estimate that in less than a decade this interconnectivity will involve as many as thirty-seven billion intelligent devices, all connected and communicating.[3] Consumers already use mobile phones to monitor home security,[4] adjust thermostats, change television channels,[5] unlock cars,[6] and remotely report a person's vital signs to their physicians for monitoring.[7] These connected devices communicate on multiple levels, both overtly and covertly. In the process, they also collect unimaginable volumes of data—both needed and not needed, harmless and highly sensitive. This data will flow to a wide range of recipients, including government agencies, corporations, researchers, health care providers, or even other consumers, who can then measure how even the most mundane of activities compares with that of others. These data trails have become our fingerprints, the record of personal and corporate decisions, and a permanent memorial to both our successes and mistakes.

Technology empowers us in ways that were unimaginable a few generations before, and our dependence on it also creates new vulnerabilities. When this tension creates a rupture between the individual's empowerment and the vulnerabilities of technology use, the ensuing disputes often land in courts. And thus, the courts take on the task of untangling the interplay between technology and fundamental issues of privacy, data security, government jurisdiction, and litigation risk.

This is not a new issue. For example, when the media began to more widely use the "snap" camera in the 1880s, some perceived it as a threat to personal privacy. Then-future Supreme Court Justice Louis Brandeis lamented in 1890:

Positively 'Nutty,' CISCO BLOGS (Feb. 12, 2013, 3:19 PM), http://blogs.cisco.com/ioe/thanks-to-ioe-the-next-decade-looks-positively-nutty.

3. Evans, *supra* note 2.

4. *See, e.g.*, Eugene Kim, *AT&T Digital Life Promises Whole Home Connectivity*, PCMAG (Apr. 26, 2013, 9:57 AM), http://www.pcmag.com/article2/0,2817,2418196,00.asp.

5. *See, e.g.*, Glen Fleishman, *Thanks to Smartphone Apps, Old Remote Control Becoming Remote*, SEATTLE TIMES (Jan. 18, 2013), http://seattletimes.com/html/businesstechnology/2020148809_ptechpracticalmacxml.html.

6. *See, e.g.*, John D. Sutter, *How to Unlock a Car with a Text Message*, CNN.COM (Aug. 3, 2011, 5:21 PM), *available at* LEXIS.

7. *See, e.g.*, Pamela Lewis Dolan, *Patients Expected to Use Smartphones for Health Monitoring*, AM. MED. NEWS (Feb. 20, 2013), *available at* LEXIS.

> [P]hotographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.[8]

We still struggle with the privacy issues of taking image photography, with social media acting as today's version of the snap camera.[9] At the outset of the technology and privacy debate, despite Brandeis's eloquent advocacy for protection of the individual, courts did not immediately recognize a right to privacy that would have prohibited or limited the use of image photography for news reporting. Courts have since examined privacy rights and defined them as discrete zones bound by the specific parameters of either a written or common law.[10]

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

9. *See* Jaikumar Vijayan, *Profile Pics on Social Media Sites Pose Privacy Risks, Researcher Warns*, COMPUTERWORLD (Aug. 5, 2011, 7:05 AM), http://www.computerworld.com/s/article/9218903 (discussing the risks associated with facial recognition use based on profile photos from Facebook and LinkedIn); *see also* Amy Webb, *We Post Nothing About Our Daughter Online*, SLATE.COM (Sept. 4, 2013, 5:30 AM), *available at* LEXIS (advocating against posting photos of children on Facebook and other social media).

10. The first Supreme Court decision to fully articulate the right to privacy was *Griswold v. Connecticut*, which held that the right to privacy included the right for married couples to use contraceptives. 381 U.S. 479 (1965). In *Griswold*, Justice Douglas, writing for the Court, explained that the guarantees in the Bill of Rights have "penumbras," which must be read as creating zones of privacy. *Id.* at 484.

> The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the

Taking a leap forward, one has to wonder what Chief Justice Brandeis might have written about the panoramic photographs and "payload data" by Google as the company developed its Street View feature to complement the Google Maps service. The court case that grew out of Google's collection of payload data is but one example of the difficult task courts face in balancing the benefits and the vulnerabilities of technology—in the case of Google Maps, the convenience of an essential web feature and smartphone applications versus the excesses of massive data collection the company conducted to create Street View.

Street View, which needs little introduction, provides panoramic, street-level photographs that have been captured by cameras mounted on vehicles that drive on public roads and photograph everything (including, initially, many surprised faces). The story could have ended there, but the data collection opportunity associated with the vehicles driving through every neighborhood in the country was not lost on Google's engineers. In addition to the cameras, Google equipped the vehicles with Wi-Fi antennas and software that collected data transmitted by Wi-Fi networks in nearby homes and businesses.[11] The equipment recorded both basic, innocuous information about the Wi-Fi networks it detected, such as signal strength, as well as so-called "payload data." The payload data included personal emails, usernames, passwords, videos and documents, and other information sent over unencrypted home Wi-Fi networks that the vehicles detected.[12]

When Google was famously sued for this practice, it seemed clear, at least from the perspective of societal privacy expectations, that the collection of the payload data was inconsistent with the desire to be "let alone."[13] Criticism of Google's actions has been

> Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'

Id. This conclusion was reached despite the fact that the word "privacy" does not appear even once in the U.S. Constitution.

11. Joffe v. Google, Inc., No. 11-17483, 2013 WL 6905957, at *1 (9th Cir. Dec. 27, 2013) (amending Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013) and granting rehearing).

12. *Id.* at *1–2.

13. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("[The makers of our Constitution] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred,

swift and far reaching.[14] Courts, however, had to decide if this practice was also illegal—specifically, in relation to the Federal Wiretap Act.[15] The outcome of that analysis was not as immediately certain, as the case presented a novel question of statutory interpretation. The Federal Wiretap Act was amended in 1968 to extend the restrictions on phone tapping to tapping of electronic communications,[16] at least ten years before the Internet and web browsers began making significant appearances in the consumer market.

Google's argument was that payload data was exempt from the general wiretapping prohibition—specifically, under an exemption for "radio communications" and another one for other "electronic communications" that are "readily accessible to the general public."[17] Google asserted that the payload data it collected met one or both of the exceptions because unscrambled and

as against the government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men.").

14. *See* Catherine Bolsover, *German Foreign Minister Joins Criticism of Google's Mapping Program*, DW (Aug. 14, 2010), http://www.dw.de/german-foreign-minister-joins-criticism-of-googles-mapping-program/a-5910738-1 (describing opposition by the German Foreign Minister to Google's Street View service); *Call to 'Shut Down' Street View*, BBC NEWS (Mar. 24, 2009), http://news.bbc.co.uk/2/hi/technology/7959362.stm (detailing complaints filed by Privacy International to the Information Commissioner); Elinor Mills, *Google's Street-Level Maps Raising Privacy Concerns*, USA TODAY (June 4, 2007, 11:53 AM), http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm (characterizing Street View as a threat to an individual's privacy).

15. Individuals whose data had been collected filed class action lawsuits against Google under the Federal Wiretap Act, 18 U.S.C. § 2511 (2012), California Business and Professions Code section 17200, and various state wiretap statutes. The cases were consolidated and assigned to the Northern District of California. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067 (N.D. Cal. 2011), *aff'd sub nom. Joffe*, 2013 WL 6905957. Google responded by filing a motion to dismiss, stating that its collection of payload data did not fall within the scope of the Wiretap Act's prohibition of the interception of electronic communications. *Id.* at 1084. The district court denied Google's motion. *Id.* At Google's request, the district court certified the question for an interlocutory appeal under 28 U.S.C. § 1292(b). *Joffe*, 2013 WL 6905957, at *2.

16. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)).

17. *Joffe*, 2013 WL 6905957, at *2 (citing 18 U.S.C. § 2511(2)(g)(i)).

unencrypted Wi-Fi signals were electronic "radio communications" that anyone—not just Google—could intercept.[18]

The Ninth Circuit Court of Appeals rejected Google's position and affirmed the district court's decision to dismiss Google's motion.[19] The court of appeals disagreed with both of Google's arguments. Although the Federal Wiretap Act does not define "radio communications," the court held that the plain meaning of that term excludes data transmitted over a Wi-Fi network.[20] The Ninth Circuit concluded that, for purposes of the Federal Wiretap Act, a "radio communication" is a predominantly auditory broadcast, and does not include other types of signals transmitted over radio waves (e.g., Wi-Fi signals).[21] The court rejected Google's argument that payload data was "readily accessible to the general public."[22] While it acknowledged that Google was able to intercept payload data transmitted over an unencrypted Wi-Fi network, the court was not convinced that this fact made the data "readily accessible" for purposes of the exceptions contained in the Federal Wiretap Act.[23]

The Ninth Circuit's decision on the meaning of the Federal Wiretap Act exemptions could have gone either way and is a prime example of the challenge courts face in benchmarking modern technology against older laws passed before the technology existed or was well known. At the time the Federal Wiretap Law was passed, most people lacked the ability to communicate by email, let alone intercept that communication with a passing vehicle. Use of radio waves was largely limited to audible communications, which could be intercepted by an amateur radio hobbyist. The court concluded that it was not foreseeable when the Federal Wiretap Act was passed that a radio hobbyist or anyone else would use technology to intercept payload data, such as emails containing personal

18. *Id.* at *2, *5. Google's arguments focused on the specific language in the Wiretap Act exempting "radio communications" that were "readily accessible to the general public." *See* 18 U.S.C. § 2511(2)(g)(i).

19. *Joffe*, 2013 WL 6905957, at *5.

20. *Id.* at *6.

21. *Id.* at *7.

22. *Id.* at *5.

23. *Id.* at *9 (noting that traditional radio services can be easily and mistakenly intercepted by radio hobbyists, but that radio hobbyists "do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks").

information exchanged between an individual and their "doctor, lawyer, accountant, priest or spouse," or communications from an unencrypted Wi-Fi network operated by a police department.[24] Accordingly, the law's exemption was inapplicable to this application of newer technology.

The Google decision is only one example of how the legal system addresses issues inherent to evolving technology, and one that may well be quickly rendered obsolete by the pace of this evolution. While we may be unable to envision at this time all of the technology innovations to come, we can reasonably predict that its advancement will continue to challenge the meaning of the Federal Wiretap Act and many other laws—whether formal discovery rules or the statutes that seek to govern technology and its byproducts. Keeping this uncertainty in mind, the authors of this volume bravely take on the challenge to provide guidance on a cross section of legal requirements and technologies that challenge the legal status quo, such as the always-critical e-discovery, legal issues arising from Google's extraction and use of individual user data, mobile payments, and cyber warfare.

By the time this volume is published, there will be new NSA revelations, even newer technology, and a host of new privacy and security risks that we have not yet considered. But the importance of being current on these requirements cannot be overstated. As I am finishing this foreword, my mind begins to shift gears in anticipation of watching the last episode of the critically acclaimed TV show Breaking Bad. Had I not seen the entire run of the show, this last episode—which I know will be memorable—would be lost on me; I would neither enjoy it nor understand it. So when the "new episode" of technology developments comes along, the great work the authors have done here will have taken you through the prior "seasons" and given you the tools to comprehend and digest the legal implications of whatever awaits us.

24. *Id.*