Journal of Technology Law & Policy

Volume XVI – Fall 2015

ISSN 2164-800X (online)

DOI 10.5195/tlp.2015.184

http://tlp.law.pitt.edu

Foreword

Daniel Harris Brean

Foreword

Daniel Harris Brean*

Privacy and technology issues tend to implicate one another. Sometimes they reinforce each other, such as when improved data security thwarts hackers. But often the use of technology diminishes privacy because, in order to benefit from the technology, users must surrender some personal, otherwise private information. In such cases the technology may be powerful, profitable, fun, or convenient, but the privacy consequences of its use can be quite profound.

The Internet, for example, provides a platform through which individuals can interact socially, professionally, and commercially on a scale like never before. We can make friends and find dates online, strictly limiting how much personal data we reveal in the process. We can speak our minds anonymously in various forums, using aliases to avoid unlawful retaliation. We can play online multiplayer games using avatars, such that one's age, sex, and other personal characteristics are irrelevant to the exercise. From this perspective, the Internet offers many new and exciting services while enhancing privacy and safety. But the same anonymity controls can be used by malicious actors such as cyber-bullies and other predators to shield themselves from adverse consequences. This begs the question of just how much privacy we are willing to tolerate online.

Taking full advantage of all the conveniences and services available online requires one to volunteer a great deal of what would otherwise be private information. Facebook knows your political leanings based on what you have read or liked in the past,[1] and even knows when you are probably going to break up with

* Daniel Harris Brean is an intellectual property attorney at The Webb Law Firm in Pittsburgh, PA, where his practice focuses on patent litigation with an emphasis on appeals. He received his BS in Physics from Carnegie Mellon University and his JD *cum laude* from the University of Pittsburgh School of Law. He is a former law clerk to the Honorable Jimmie V. Reyna at the United States Court of Appeals for the Federal Circuit. He is also an adjunct professor, teaching patent law, at the University of Pittsburgh School of Law.

Author's Note: As the former lead articles editor of this journal, now teaching at Pitt, I am delighted to introduce this edition. The provocative topics, engaging writing, and high-quality scholarship brought to you by this array of authors is truly excellent. I thank the editorial board and staff, and Paul Coury and J. Darwin King, Jr. in particular, for inviting me to set the scene for you with this foreword.

[1] https://www.yahoo.com/tech/facebook-already-knows-who-youre-voting-for-101193029189.html.

Journal of Technology Law & Policy

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.184 ● http://tlp.law.pitt.edu

your significant other.[2] Apple knows when you are getting into your car, where your next meeting is, and tells you how long it will take you to get there.[3] Amazon will soon know when you are running low on detergent or dog food and will order more of it for you.[4] If you use Google's Chrome browser, Gmail email service, and Google Maps program, Google knows where you are, what you do, what media interests you, who you talk to, what you buy, and many, many other pieces of information that allows Google to specially target content, products, and services to you.[5] And many of these services cross-collaborate their data about you with each other, using your information to offer even more robustly customized experiences for you. Whether such value-added services are good or bad, they confirm that a wealth of private information is being given to, and used by, third parties at a staggering rate. Very few Internet users are acutely aware of how broadly their information is being utilized and shared, making this surrender of private information both voluntary and, in a sense, involuntary (or at least ignorant). This begs the question of just how little privacy we are willing to tolerate online.

In my field of patent law, which is charged with promoting technological progress, the presence or absence of privacy and secrecy also plays critical roles. The cornerstone of the patent system is the idea that a complete public disclosure of a meritorious (i.e., patentable) invention will entitle the inventor to a strong property right in that invention. As such, one cannot keep to oneself the best mode of an invention but also seek to patent it, and one's disclosure of an invention to the U.S. Patent and Trademark Office must be sufficiently detailed to enable another in the field to make and use the invention.[6] At the same time, we generally measure the merits of an invention against what was publicly known or knowable, not what was secret.[7] Although historically secret commercialization of an invention would adversely affect later attempts at patenting,[8] recent patent reform requires such

[2] http://nypost.com/2013/10/29/facebook-knows-when-youre-going-to-break-up/.

[3] http://www.cnet.com/how-to/how-to-turn-off-ios-9s-automated-traffic-helper/.

[4] http://www.azcentral.com/story/money/business/consumer/2015/03/31/amazon-gadgets-make-ordering-easy-automatic/70750650/.

[5] http://www.digitalinformationworld.com/2015/04/how-much-does-google-really-know-about-you-infographic.html.

[6] 35 U.S.C. § 112(a) (2012).

[7] 35 U.S.C. § 102(a)–(b) (2006) (providing that an invention is not patentable if, *inter alia*, it was "known or used by others in this country, or patented or described in a printed publication," or "in public use or on sale in this country").

[8] 35 U.S.C. § 102(a)–(b) (2006); Metallizing Engineering Co. v. Kenyon Bearing & Auto Parts Co., 153 F.2d 516 (2d. Cir. 1946).

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.184 ● http://tlp.law.pitt.edu

activities to be public in order to affect prospective patent rights.[9] Even the ownership and control of patent rights is shifting toward more transparency, with bills in Congress seeking to require identification and joinder of interested parties in patent litigation.[10]

Almost every doctrine and policy in patent law reflects a careful balancing of enriching public knowledge vs. incentivizing private innovation. The optimal results should encourage innovation without unduly prejudicing the public. In many respects, I believe this parallels the need to weigh the benefits of technological advancement against the erosion (voluntary or otherwise) of privacy rights. In this context, the question must be whether we are encouraging adoption of technology that makes us and our data more usable, beneficial, and secure, while at the same time being responsible to users and respectful of users' privacy rights.

This edition of the *Pittsburgh Journal of Technology Law and Policy* is loosely themed around the notion of "private technology," and some version of this balancing act is what most of these authors sought to perform. The articles explore complex questions of law and policy arising out of the intersection between technology and privacy, in contexts such as data security, metadata, law enforcement, and automotive safety. The following is a short preview of this edition's contents.

Data security and responsible data usage is at or just under the surface of any discussion about how privacy and technology can be appropriately balanced. This edition examines data security and usage challenges from many angles, including: (1) whether the computer and software usage by K-12 students at school requires enhanced protection against abusive and commercial uses by third parties; (2) whether states are doing enough to protect against and punish those responsible for so-called "revenge porn"; (3) whether, in light of the number of recent hacks of companies' databases that exposed countless individuals' personal and identifying information, those hacks could have been prevented or their damage minimized, and what additional protections should be in place; (4) whether the so-called "right to be forgotten" should be recognized more broadly to allow individuals to have online information about themselves removed due to irreparable reputational harm; and (5) whether appropriate statutory incentives are in place for the adoption and usage of electronic health records. These articles initiate important conversations about the

[9] 35 U.S.C. § 102(a) ("A person shall be entitled to a patent unless—(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, *or otherwise available to the public* before the effective filing date of the claim invention").

[10] http://www.patentprogress.org/patent-progress-legislation-guides/patent-progresss-guide-patent-reform-legislation/.

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.184 ● http://tlp.law.pitt.edu

proper collection, maintenance, and usage of one's data, as well as what to do when those responsible for keeping data private or secure fail to do so.

Metadata—the information underlying an electronic document, including a record of previous changes and edits to the document—presents some interesting and unique issues of data security. Metadata is in a sense hidden and private, and not usually intended to be shared with a recipient of a final version of the document, though it is capable of being "scrubbed" or removed by the creator of a document or "mined" and extracted by the document's recipient. One article in this edition questions whether metadata should be presumptively provided by the government in response to Freedom of Information Act Requests, concluding that, absent a legitimate national security concern, metadata generally should be disclosed in the spirit of government transparency and accountability. Another article explores the ethical concerns that arise when the metadata of a document is mined and used by attorneys, finding that the context (discovery or not) and the nature of the information (confidential or not) leads to different ethical conclusions.

Technology and privacy concerns also often collide in the law enforcement context, where the reliability and invasiveness of technologies used to assist police officers must be carefully weighed against constitutional privacy rights. One article in this edition examines the current usage of body cameras on police officers, concluding that the accountability and clarity of the record of police conduct can beneficially protect the police and the public, but that the lack of clear policies for usage of the cameras and access to the footage could undermine the value and efficacy of body camera programs in the criminal justice system. Another article details how a person's microbiome (essentially, a "germ cloud"), which is as unique as one's DNA, may be far more effective for tracking and catching criminals than DNA, but raises additional privacy concerns because one's microbiome reveals personal information (e.g., drug habits, race, sexual orientation) not detectable via DNA.

Cars continually adopt and incorporate new technologies, and vehicle data tracking with network connectivity is becoming more common. Two articles in this edition explore whether vehicle-to-vehicle communication and alerts concerning a car's position, speed, and direction will increase or decrease safety on the roads. One concludes that it will increase safety, but notes that regulatory relinquishment of frequency spectrum will be instrumental to achieving this goal. The other demonstrates how the technology may make drivers less safe, and examines the increased complexity of personal injury litigation in such accidents where the manufacturer's vehicle-to-vehicle communication system is allegedly partially responsible for accidents.

Detailed discussions of these and other fascinating issues await you in the following pages. On behalf of the entire Pittsburgh Journal of Technology Law and

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.184 ● http://tlp.law.pitt.edu

Policy, as well as the authors of this edition, I invite you to ponder whether each form of technological progress justifies the corresponding privacy and security drawbacks. If it does not, do we need better technology, better laws, or better values?

Volume XVI – Fall 2015 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2015.184 ● http://tlp.law.pitt.edu