4-1-2015

Internet of Things: A Privacy Law Case Study

Sarah McMahon

Internet of Things: A Privacy Law Case Study

Sarah McMahon[1]

Abstract

The typical law school seminar contains a set of readings, accompanied by a series of session-specific introductions and "notes & questions" to help structure class discussion. This document provides a comprehensive set of materials for such a seminar, on a fourteen-week calendar, that explores privacy law through the lens of the new technologies popularly known as "the Internet of Things" (IoT). Indeed, two of the most discussed topics in the legal profession right now are privacy law and the implications that IoT may have on data privacy and security. By examining major topics in privacy law while paying special attention to the implications of IoT devices, this seminar provides a unique format for analyzing and studying a topic as broad and storied as privacy law. Created as an independent study project by a third-year law school student, this "seminar in a box" document provides all of the reading lists, introductory materials, and discussion questions needed to conduct this topical seminar. A professor might use this document or portions of it in her classroom, or a student may find this resource useful as a starting point for further research. A central aim of this project is to provide a useful introductory guide to privacy law.

[1] J.D., University of Georgia School of Law.

Introduction

Privacy is undoubtedly one of the most significant legal topics of our time. We encounter privacy policies with virtually every online product or service, and new technologies not only provide recreational or health benefits to consumers, they also aid the government in their surveillance efforts, as well as criminals in their illegal activities. Further, the Internet of Things (IoT), or the phenomenon of devices communicating with us and with each other, is already here with common wearable devices, and it will only grow in the coming years. The privacy implications that this vast array of technologies presents are endless. This document examines privacy law through the lens of the Internet of Things, because as technology advances at an ever-increasing rate, with each new advancement, we find ourselves reevaluating our privacy rights, interests, and expectations.

Importantly, this document is not a typical law school research paper about privacy law and technology. Instead, I approached my goal of learning about the topic of privacy law in a different way. With the guidance and support of Professor Joseph Miller of the University of Georgia School of Law, I created a seminar that can be taught in any law school. In this document, I provide a comprehensive set of materials for fourteen two-hour seminar classes. Each class session has a reading list, introductory material, and discussion questions based on the reading list for that class. For each session, I have also included one or more suggested further readings, to help students interested in a particular topic dig further into it.

My methodology for choosing the layout of the course began with an examination of the tables of contents in leading privacy scholars' textbooks to see what the major subtopics of privacy law were and how they could be assembled in a logical way.[2] After creating a general outline of my own, taking inspiration from those existing frameworks, I did more focused research on specific topics to find and read relevant articles, cases, and statutes, all while paying particular attention to how topics related to developing technology and digital privacy. I wrote the discussion questions after determining the goal

[2] Daniel J. Solove & Paul Schwartz, *Privacy, Information, and Technology*, 3rd Ed. (2011); Daniel J. Solove & Paul Schwartz, *Information Privacy Law*, 4th Ed. (2011).

of each class, reading each assignment thoroughly, and discussing the readings with Professor Miller.

Instead of writing a paper on a very narrow perspective of the intersection of privacy law and IoT, I opted to find a unique way to tackle an entire subject area in one semester by recreating a law-school seminar with a fictional classroom and myself as the professor, researching the law and encouraging lively discussion on the various topics. I hope this project will be a valuable resource for those who aim to learn more about this exciting area of the law.

I. Background & Overview

Session 1. *History & Perspectives*

Before delving into the specific ways that Internet of Things technologies and privacy law may affect one another, we must first better understand the historical, sociological, and academic perspectives that have shaped the development of this vast legal arena. One way to accomplish this broad level of understanding is to examine the development of privacy law in the tort context. Privacy law evolved, in part, from the need to respond to new technologies that emerged over a century ago, much like the advent of the Internet of Things we experience today. Additionally, by identifying the basic characteristics of tort law (rights, responsibilities, harms, and remedies) in the privacy context, we begin to paint the broader landscape of privacy law. For instance, to identify privacy injuries and duties, we inevitably must discuss the nature of those injuries (Is the harm emotional? Financial? Both?), and how they might differ based on human relationships and expectations of confidentiality.

A discussion of privacy tort law is not complete without an introduction to the theories of Samuel Warren, Louis Brandeis and William Prosser, who are arguably the most influential figures in this area of law. Warren and Brandeis influenced over half a century of privacy law development with their 1890 article that advocated for legal recognition of an inherent right to be left alone. Prosser was certainly more influential, however, as his treatises, casebooks, and especially his 1960 law review article shaped modern privacy tort law into the four privacy torts that still exist today. Additionally, underlying all of the academic discussions on privacy law is the sociological concept of the public-private distinction, in which a person has an impenetrable life and chosen personality at home and a separate persona and set of expectations for life in public. The exploration of privacy torts, along with an examination of relevant historical and sociological circumstances, will thus provide a basis of knowledge necessary to discuss privacy in other legal contexts, such as medical privacy or privacy from government intrusion.

Notes & Questions

Public-Private Distinction

1. How would you describe how our society thinks of public and private spheres? Does your categorization differ from the four ways that Weintraub says public and private spaces are currently distinguished?
2. Weintraub argues that use of the term "privacy" is limited as a signal for things that we want to "keep hidden, sheltered, or withdrawn from others." Is this a fair assessment of how we think of privacy today? Or is our concept more fluid than a strict dichotomy between public and private spaces?

Key Figures: Warren, Brandeis, and Prosser

3. In what ways did the public-private distinction influence Warren and Brandeis in their 1890 *Harvard Law Review* article?
4. In their article, Warren and Brandeis point to developments in technology as the central reason that the law needed to adapt and better recognize one's right to be let alone. What parallels can you draw between the historical moment of technological change that Warren and Brandeis were experiencing and the current technological precipice on which we find ourselves today?
5. Warren and Brandeis's article was an innovative and persuasive piece of writing, due in no small part to the way they constructed their arguments. How would you articulate their process of advocating for the right of privacy, and how might this method be applied to the current state of the law and technology?
6. In "Mainstreaming Privacy Torts," Citron describes both the Warren and Brandeis model for conforming privacy law to fit modern privacy harms as well as Prosser's ultimately more influential approach. Which of the two approaches is more convincing to you, and why? Do the benefits of Prosser's four strict categories outweigh the innovative Warren and Brandeis approach? If Prosser's four privacy torts had not won over practitioners and judges, how might Warren and Brandeis's model have continued to develop? In other words, how would (or could) Warren and Brandeis's theories apply to the emerging technologies of today?

Privacy Law: Present and Future

7. Citron points out various types of actors who might cause the multitude of privacy harms that exist in the digital age (from individuals, to governments, to business entities). What possible actors, injuries, and new technologies were most surprising to you? Do her solutions for privacy tort reform adequately address each of these actors and injuries?
8. Citron believes that confidence law is "an underutilized resource for today's privacy problems." Is the breach of confidence claim undermined by our current climate of frequent data breaches and decreased expectations of privacy, especially in public spaces? In other words, how confident can we reasonably be that people with whom

we share our private information (including business entities, individuals, and the government) will keep that information in confidence?

9. Virtually nowhere in any of the three assigned readings is the role of the legislature mentioned. Where should, and where could, legislation be effective? How might the formula created by Prosser and the one created by Warren and Brandeis work in statutory format? Do you know of any legislation that addresses privacy concerns, and if so, how does it work?

Reading List

1. *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy*, University of Chicago Press (1997).
    i. p. 1-7 of chapter 1, "The Theory & Politics of the Public Private Distinction" by Jeff Weintraub.
2. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, **193-208** (1890).
3. Danielle K. Citron, *Mainstreaming Privacy Torts*, 98 Cal. L. Rev. 1805 (2010)

Suggested Reading

1. *Sidis v. F-R Pub. Corp*., 113 F.2d 806 (2d Cir. 1940)
2. Aimee Jodoi Lum, *Don't Smile, Your Image Has Just Been Recorded on A Camera-Phone: The Need for Privacy in the Public Sphere*, 27 U. Haw. L. Rev. 377 (2005)
3. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887 (2010)

Session 2. *Big Data & the Internet of Things*

The previous section introduced foundational theories of privacy law from an historical perspective. This section begins to connect those concepts with the privacy law implications of Internet of Things technologies. This introduction provides working definitions of the Internet of Things and the inextricably linked concept of Big Data. Additionally, this introduction provides some background on the Federal Trade Commission, which uses its broad consumer-protection mission to regulate many aspects of consumer technology.

The "Internet of Things" is just one of many ways to describe the phenomenon of devices communicating with us and with each other.[3] The IoT is comprised of the various possible connections between and among people and objects.[4] In other words, devices use sensors to record information about people or objects, and then those devices connect to each other via a network, communicate across different programming languages, and even begin to analyze collected data, which can then be transmitted back to people or other devices.[5] Existing IoT products include wearable technologies like the fitness devices Fitbit and Jawbone, which can track steps, sleep habits, and heart rate, and transmit that data to another device. IoT technologies are not limited to health products or even consumer-facing products; they include industrial applications as well.[6]

Like IoT, the concept of "Big Data" has many possible definitions. In essence, Big Data is the phenomenon of large volumes of information created by and about people and technologies, given that "data is now available faster, has greater coverage and scope, and includes new types of observations and measurements that were previously not

---

[3] See Sanford Reback, "Deconstructing the Internet of Things," Bloomberg Government Analysis, Oct. 29 2014, page 1, available at http://op.bna.com/pl.nsf/id/kjon-9qdjys/$File/Deconstructing%20the%20Internet%20of%20Things.pdf. To put it another way, IoT is "a network of devices where all of the devices (1) have local intelligence, (2) have a shared API [(application program interface)] so they can speak with each other in a useful way, even if they speak multiple protocols, and (3) push and pull status and command information from a networked world." Kipp Bradford, "The Industrial Internet of Things," Forbes, Feb. 5, 2014.

[4] Jacob Morgan,"A Simple Explanation of the Internet of Things," *Forbes* May 13, 2014, available at http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/. This article also has an interesting visual aid to illustrate a world with IoT.

[5] *See Id. and* Rakesh Sharma, "A New Perspective on the Internet of Things," *Forbes.com*, Feb. 18, 2014.

[6] *See* "Internet of Things Examples," *Postcapes.com*, available at http://postscapes.com/internet-of-things-examples/ (last accessed: Jan. 31, 2015).

available."[7] The data generated by people and devices within the Internet of Things is a crucial contribution to the present and future state of the Big Data phenomenon, but it is not the only contribution. A comprehensive overview of Big Data's evolution is not possible here. That said, as we study key IoT technologies and related privacy harms, it is important to keep in mind how they coexist with Big Data privacy concerns and developments, given that Big Data technologies, including IoT, "can derive value from large datasets in ways that were previously impossible."[8]

The Federal Trade Commission is a federal agency with dual goals of protecting consumers and promoting competition—specifically, to "prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity."[9] The FTC has the authority to enforce and administer a variety of laws, including consumer protection laws "that prevent fraud, deception, and unfair business practices," as well as federal antitrust laws that prevent anticompetitive business practices.[10] The agency can conduct investigations, sue companies and individuals, and promulgate binding rules.[11] The range of activities that fall within the FTC's domain is vast, because any kind of business can be subject to the agency's consumer protection authority or its competition promotion authority.

Because of its broad purpose and comprehensive enforcement power, it is important to examine the FTC's work when determining how existing laws may address privacy concerns arising from IoT technologies. Specifically, we can see how a consumer's expectation of privacy is jeopardized when he does not know how, or even if, data from his devices is being collected by a company or an unknown third party. The FTC naturally takes interest in widespread consumer dissatisfaction with goods or services that consumers

[7] "Big Data: Seizing Opportunities, Preserving Values," report to the White House, 2014 (citing Liran Einav and Jonathan Levin, "The Data Revolution and Economic Analysis," Working Paper, No. 19035, National Bureau of Economic Research, 2013, http://www.nber.org/papers/w19035; Viktor Mayer-Schonberger and Kenneth Cukier,Big Data: A Revolution That Will Transform How We Live, Work, and Think, (Houghton Mifflin Harcourt, 2013).
[8] *Id*.
[9] http://www.ftc.gov/about-ftc
[10] http://www.ftc.gov/enforcement
[11] http://www.ftc.gov/about-ftc/what-we-do

find to be far more intrusive than marketing materials led them to expect.[12] Additionally, the FTC is uniquely situated as regulator, in that it must strike a balance between protecting consumers from deception and promoting vigorous competition.

Notes & Questions

1. In his book *Understanding Privacy*, Daniel Solove proposes the following taxonomy regarding groups of harmful activities in privacy law: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.[13] Which of these harms does the January 2015 FTC Staff Report on the Internet of Things address most sufficiently? Who are the possible persons or parties who might inflict these harms, or receive them? What are the ways that such privacy harms are inflicted?
2. Can you think of a good or service that you have used recently that gave you a choice about your data, through an option such as an end-user license agreement or terms and conditions? Did you read the option or accept without reading? What would you expect to be covered in such a document?
    a. Below is an excerpt from the privacy policy of an IoT health tracking device, the Fitbit. Is it aligned with your expectations about this device? Do you think the definitions of Personally Identifiable Information and De-identified Data are adequate? If not, how would you modify them?

> **Data That Could Identify You**
> Personally Identifiable Information (PII) is data that includes a personal identifier like your name, email or address, or data that could reasonably be linked back to you. We will only share this data under the following circumstances:
> - With companies that are contractually engaged in providing us with services, such as order fulfillment, email management and credit card processing. These companies are obligated by contract to safeguard any PII they receive from us.
> - If we believe that disclosure is reasonably necessary to comply with a law, regulation, valid legal process (e.g., subpoenas or warrants served on us), or governmental or regulatory request, to enforce or apply the Terms of Service or Terms of Sale, to protect the security or integrity of the Fitbit Service, and/or to protect the rights, property, or safety of Fitbit, its employees, users, or others. If we are going to release your data, we will do our best to provide you with notice in advance by email, unless we are prohibited by law from doing so.
> - We may disclose or transfer your PII in connection with the sale, merger, bankruptcy, sale of assets or reorganization of our company. We will notify you if a different company will receive your PII and the promises in this Privacy Policy will apply to your data as transferred to the new entity.
>
> **Data That Does Not Identify You (De-identified Data)**
> Fitbit may share or sell aggregated, de-identified data that does not identify you, with partners and the public in a variety of ways, such as by providing research or reports about health and fitness or as part of our Premium membership. When we provide this information, we perform appropriate procedures so that the data does not identify you and we contractually prohibit recipients of the data from re-identifying it back to you.[1]

[12] *See e.g.*, http://www.ftc.gov/tips-advice/business-center/advertising-and-marketing.
[13] Daniel J. Solove, *Understanding Privacy*, Harvard University Press (2008), p. 103.

3. The FTC Staff Report explains that an "increased focus on certain types of use restrictions" could shift responsibility "away from data subjects towards users, and [increase] the emphasis on responsible data stewardship and accountability." How does this shift in responsibility, mentioned on page 24 of the FTC Staff Report, comport with tort law, including the privacy torts we discussed in the previous section?
4. In Solove's "Access and Aggregation" article, he proposes that the nature of the pertinent harm is the "aggregation problem" that "arises from the fact that the digital revolution has enabled information to be easily amassed and combined." (p. 1185). How would you characterize harms "digital biographies"? What are the possible benefits from such inferences from our data?
5. We have begun to identify the various kinds of privacy harms and the individuals who may receive or inflict such harm in the context of the Internet of Things; we have learned about the limitations and possibilities of IoT technology; and we have read how others believe the law should develop in this area. With this background in mind, how would you structure legislation to address privacy concerns and IoT? Would you need a separate scheme for different contexts, such as medical privacy versus consumer credit transactions? Or would you want a single unified approach to address the issue at a sufficiently general level?

Reading List

1. "Internet of Things: Privacy & Security in a Connected World," FTC Staff Report, January 2015.
2. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1184-1195 (2002).

Suggested Reading

1. Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 Wake Forest L. Rev. 393 (2014)
2. Richards, Neil M. and King, Jonathan H., *Big Data and the Future for Privacy* (October 19, 2014). Available at SSRN: http://ssrn.com/abstract=2512069 or http://dx.doi.org/10.2139/ssrn.2512069.

Session 3. *Legislation*

In previous sections, we connected fundamental privacy theories with both the concept of Big Data and emerging concerns about Internet of Things technologies. Here, we see how such concepts work in two crucial pieces of federal privacy legislation, in order to show the (dis)connect between existing law and both IoT technology and fundamental privacy theories. The two pieces of major legislation are the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Fair Credit Reporting Act of 1970 (FCRA).

Among other things, HIPAA regulates how qualifying health-related entities can use, store, and disseminate health information. The Office of Civil Rights within the U.S. Department of Health and Human Services enforces specific rules of HIPAA, such as The Privacy Rule, "which protects the privacy of individually identifiable health information," and The Security Rule, "which sets national standards for the security of electronic protected health information."[14] An interesting aspect of this enforcing body is that the HIPAA guidance that it has published was, like HIPAA itself, written well before smart phones and tablets existed. As a result, any average citizen or practitioner who seeks advice today will not necessarily get specific guidance for emerging technologies.[15]

The Federal Trade Commission enforces FCRA. Congress enacted FCRA in 1970 to encourage both accuracy and fairness of credit worthiness evaluations and respect of consumers' right to privacy, as credit reporting agencies assemble consumer information.[16] To this end, FCRA regulates how consumer reporting agencies access and use consumer information.

Both HIPAA and FCRA are appropriate vehicles through which one can practice applying existing laws to emerging technology in the privacy law context, because both statutes address vital but very different aspects of individual privacy. HIPAA protects an individual's health information to the extent it might represent that person's personal

[14] www.hhs.gov/ocr/privacy/
[15] See "Summary of HIPAA Privacy Rule," United States Department of Health and Human Services (last updated in May 2003).
[16] 15 U.S.C. § 1681(a). The FCRA has since been amended by various acts like the Fair and Accurate Transactions Act of 2003 and the Consumer Financial Protection Act of 2010. *See* FTC Staff Report "Fair Credit Reporting Act," (September 2011) page 3, available at: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf.

identity, while FCRA protects an individual's transactional consumer information to the extent credit reporting agencies and others might improperly use it. By using statutory text and official guidance to answer concrete questions about a particular technology, one can begin to appreciate the unavoidable difficulty that legislatures have in writing a comprehensive law that aims to successfully adapt to unpredictable changes in technology and in privacy expectations. As you work through the hypothetical and questions below, think about how each act approaches key aspects of the right to privacy, from the nature of the privacy harms to the people or entities capable of committing those harms, and note the similarities and the differences.

Notes & Questions

Hypothetical Scenario

Imagine that Apple, one of the largest technology companies in the world, has just developed a ground-breaking new wearable device called the iSwatch. The "iSwatch" has many new features, including the ability to track health data. Such tracking technology includes the basics like an accelerometer and pedometer to track exercise and movement throughout the day, a heart-rate monitor, and a sleep-tracker. In addition to these somewhat standard wearable health-technology features, Apple has created sensors and software to automatically track what you eat (with nutritional values and portions) and when you eat it, so that you can have an easy and comprehensive way to know every aspect of your health. Before this revolutionary technology, you could use free apps to manually input this information, but now the iSwatch makes your life easier by eliminating the need to do this. All of this health-related data, from the number and type of steps you take to what food you eat, is stored both on the device itself (which looks a lot like the new iWatch) as well as on the "iCloud," which is an online storage space accessible using your Apple ID and password on any kind of device, even via an internet browser on a traditional computer. Additionally, this health information is automatically sent to your doctor, nutritionist, health insurance, or other health professionals, because you input all of that information when you set up the iSwatch. This way, your total health profile can be analyzed and tracked, all with the hope of improving your overall health and fitness lifestyle.

In addition to these health aspects and many other useful features, the iSwatch also provides a solution to life's daily problem of keeping up with a wallet and many forms of payment. The iSwatch utilizes a new technology called iPay, which is a near-universally accepted form of payment that is similar to, but separate from, major credit cards like Visa or American Express. The way it works is that you just scan the screen of the iSwatch at any participating retailer, and money is charged to your iPay account. You get a monthly statement from Apple and pay this off using your bank account, just like you would with a traditional credit card company. The data about your transactions and payment history is stored both on the device and in the iCloud.

Your friend Jim thinks this new device is perfect for him, so he rushes out and gets the iSwatch, wearing it day and night. Over the next few weeks, the device tracks Jim's health data, and he uses the device to pay for many items because it's just so fun and easy to use, plus it gives him a chance to show off this amazing technology. Unfortunately, after a successful few weeks of showing off his watch, it begins to get the wrong kind of attention: a thief, someone Jim doesn't know at all, steals his iSwatch. The police are still searching, but it looks like there is no way he will get that device back. To make matters worse, it looks like the thief found a way to access Jim's iCloud *and* his iPay information! The thief has made many fraudulent charges on his iPay account and is completely ruining his health stats with his bad eating habits, which might put at risk his credit score and his health insurance premiums (his health insurance awards Jim for good health).

Jim is in shock that someone could have access to such personal information about him just by getting a hold of the device. As Jim's friend, you agree to help him scour the internet for resources to find a way to sanction Apple and anyone else who might be responsible for betraying his trust and leaking his personal information in this way. Look over the HIPAA and FCRA materials and answer the following questions to see if they will help Jim's cause:

1. Is Apple covered by the HIPAA Privacy and/or Security Rule? If so, what information is protected?
2. Does the iSwatch have sufficient technical safeguards according to § 164.312? If not, how might the iSwatch technical safeguards be modified to be compliant with this HIPAA Security Rule?

3. Under the FCRA, what can you do now that your iSwatch and associated iPay account have been stolen and have wreaked havoc on you credit score?

Reading List

Health Insurance Portability and Accountability Act

1. "Summary of HIPAA Privacy Rule," United States Department of Health and Human Services, (last revised May 2003) available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last visited May 8, 2015).
2. HIPAA Security -- 45 CFR §§ 164.306 and 164.312
3. HIPAA Privacy – 45 CFR § 164.502

Fair Credit Reporting Act

1. "Summary Of Your Rights Under The Fair Credit Reporting Act," Federal Trade Commission, available at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf (last visited May 8, 2015).
2. Requirements relating to information contained in consumer reports -- 15 U.S.C. § 1681c
3. Disclosures to consumers – 15 USC § 1681g

II. Personal Privacy

Session 4. *Privacy of Identity*

In this section, we explore what controls someone might expect to have over information that relates specifically to one's identity. These include the ability to omit identifying information – control over anonymity – and the ability to delete inaccurate or undesirable information online – reputational control. The right to be anonymous is the right to choose not to associate your identity with something, online or not online. The right to be forgotten, on the other hand, relates strictly to your online presence, either as you have created or as other entities might publish. Might the fundamental theories supporting a privacy right extend to these aspects of your identity, or must you be resigned to accept that you, and in particular your online presence, will be partially out of your control?

Notes & Questions

1. In his article "Anonymity as a Legal Right: Where and Why it Matters," Martin Fargo introduces case law that showcases a balancing of rights and interests, as laws intended to protect identity inadvertently run up against First Amendment concerns. (p. 330). This tension creates a kind of battle of the privacy interests—whose rights are more important, the speaker's first amendment rights to express opinions on someone, or the subject's right to privacy, in the form of his interest in not being defamed? How should these interests be balanced?
2. How might the shield laws that Fargo introduces in his article, and that protect journalists' confidential sources, work in the emerging Internet of Things framework? (p. 335-36). Would devices used by journalists need special protection or software to protect sources?
3. Meg Ambrose in her article "It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten," acknowledges that "*everyone* is potentially a data controller" and potentially subject to laws that demand removing information online. This conundrum, as with the right to anonymity, creates another battle of privacy rights: you expect certain freedoms of expression online, but must balance

these expectations with a potential right to be forgotten. While the EU Commission proposes exceptions (p. 383) that attempt to balance these important considerations, there still must be a weighing of interests. Whose interests are more worthy of protection, and what is the proper balance between these interests? Do you agree with the scholars who argue that "information asymmetry must be addressed with a "right to delete" because of a need to shift power from the data controller to the user. (p. 417).

4. A potential answer to the previous question is encapsulated in Wikipedia's policy (p. 413-414 of Ambrose article), as it implicitly acknowledges a person's right to write about individuals, and it explicitly protects the interests that private individuals have in controlling their online reputations. The policy accomplishes this balance of interests by using "notability" factors in deciding what topics may be published, such as weighing public interest in a person's identity with that individual's personal interest in controlling his reputation. Does this kind of policy strike the proper balance between free speech concerns and an individual's concern about his online reputation? What other factors should be considered?
5. In the Internet of Things, many items might not be posted for public comment per se. The collected data, however, can still be used to paint a picture of an individual's identity. How might these concepts, the right to anonymity and the right to be forgotten, interact with big data collection that occurs within the Internet of Things? Do you have a right to know or dictate how your data is analyzed, given that such analysis might change who you are? What if data collections misrepresent you in some way, or are corrupted or otherwise unreliable? Should you have a general right to have any such data deleted? What principles support this right?

Reading List

Anonymity

1. Jason A. Martin & Anthony L. Fargo, *Anonymity As A Legal Right: Where and Why It Matters*, 16 N.C. J. L. & Tech. 311, 313-50 (2015).

Reputation & the Right to be Forgotten

1. Meg L. Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten*, 16 Stan. Tech. L. Rev. 369, 371-75, 395-99, 412-420 (2013) http://stlr.stanford.edu/pdf/itsabouttime.pdf.

Suggested Reading

1. Bryan H. Choi, *The Anonymous Internet*, 72 Md. L. Rev. 501 (2013).
2. European Commission, "Factsheet on the 'Right to be Forgotten' Ruling (C-131/12)," (2012) available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited May 8, 2015).
3. European Commission, "Myth-Busting the Court of Justice of the EU and the 'Right to be Forgotten" (2014), available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_en.pdf (last visited May 8, 2015).

Session 5. *Privacy of Place*

While we might have fluctuating expectations of privacy regarding our digital identities (as we explored in the last class), shouldn't we still be able to consistently rely upon fundamental expectations of privacy in certain physical locations? As we will discover in this class session, the answer depends on where we are at any given moment. Justice Scalia observes in *Kyllo v. United States* that the interior of one's home is the "prototypical . . . area of protected privacy,"[17] particularly as protected against governmental intrusions. But what happens when law enforcement techniques advance to the point where actual *physical* intrusion is no longer necessary to understand what goes on within the privacy of a person's home? The other, albeit unstated, side of Scalia's observation is that people should not expect and should not receive such privacy protection in more public spaces. While the archetype of protected privacy is the home, how do our expectations change in quasi-public places such as school and work?

In this class session, we will discuss whether and how expectations of privacy differ depending on *where* we are, and how such different expectations affect our legal right to privacy in each location. To this end, before reading the assignment for this class, think of the key differences among the types of locations that each reading presents. Based on fundamental principles discussed in the last class regarding privacy of identity, and taking into account generally relevant countervailing public interests, how do you expect jurisprudence to have developed in the following scenarios: home, school, and work? Think of your personal experiences and your general expectations of privacy in each of these places. How do your general expectations of privacy differ depending on the place? Do your expectations affect your behavior within those environments? Are there certain aspects of each place where you expect more or less privacy; for example, a desk, cafeteria, or locker?

[17] 533 U.S. 27, 34 (2000).

Notes & Questions

1. Identify the various countervailing public interests in *Stanley*, *Kyllo*, *Safford*, and *Quon*. Which ones outweigh or support individual privacy concerns in each case? For example, while Georgia's paternalist argument did not persuade the Court in *Stanley*,[18] does the state sometimes have a public interest greater than an individual's private concerns?[19]
2. The particular thermal-imaging device is not the only technology the Court is concerned about in *Kyllo v. United States*; the majority envisioned a future with devices that can literally see through walls.[20] However, Justice Scalia is careful to limit the protection of privacy against government intrusion to devices not currently in "general public use." Might this limitation contribute to the very erosion Scalia warns about regarding minimum expectations of privacy as guaranteed by the Fourth Amendment?
3. Why did the school officials in *Safford Unified School District v. Redding* retain immunity in that case, and does such reasoning outweigh the student's Fourth Amendment and privacy interests there? Or, is Justice Stevens correct in his dissent where he says, "the clarity of a well-established right should not depend on whether jurists have misread our precedents."[21]
4. What are the fundamental differences between public employees and private employees that determine how the law treats them differently? Why did Justice Kennedy in *City of Ontario v. Quon* find that an employee's reasonable expectations of privacy were not strong enough to protect Quon against a warrantless search of his phone?[22] Are either of his two legal theories convincing, particularly given fundamental differences you thought of for public employees versus private employees? Clearly Secunda believes that the two sectors should not be treated equally in terms of the privacy rights afforded to employees, but why not?
5. Secunda discusses the distinction between an interest in privacy and an interest in autonomy in the workplace, particularly as proposed for the Restatement (Third) of Employment Law. The latest proposed draft of the Restatement, updated April 8, 2014, contains three, rather than the four outlined in the Secunda article, categories of Privacy Interests:

> This Section recognizes three distinct areas where employees have cognizable privacy interests against employer intrusions: the employee's physical person and personal physical functions and physical or electronic locations in which the employee has a reasonable expectation of privacy (§ 7.03); employee information of a personal nature (§ 7.04); and employee information of a personal nature disclosed

[18] Stanley v. Georgia, 394 U.S. 557 at 560 (1969).
[19] Note that *Stanley* does not extend to using the channels of commerce, i.e., there is no right to receive obsene materials in commerce. *United States v. Whorley*, 550 F.3d 326 (4th Cir. 2008).
[20] 533 U.S. at 35.
[21] 557 U.S. 364, 381 (2009).
[22] *See generally* Secunda, Privatizing Workplace Privacy, 88 Notre Dame L. Rev. 277 (2012) (discussing City of Ontario v. Quon, 130 S. Ct. 2619 (2010)).

> to the employer in confidence (§ 7.05). An employer intrusion into one of these three interests is necessary, but not sufficient, to find the employer liable for an invasion of privacy. In addition, the employer's intrusion must be highly offensive to a reasonable person in the circumstances in order for the employer to be subject to liability under this Chapter (§ 7.06).[23]

Recall your own work place experiences in the context of these privacy interests. Did you have a privacy discussion with your employer? Did you read through privacy policy manuals? Do such concepts match the expectations of privacy you considered in your preparation for this reading assignment?

6. While most people might think of the Fourth Amendment as the main privacy-related provision in the Constitution, we see in the cases for this session that one can use other provisions to support the fundamental right to privacy. For example, we see the intersection of the first amendment and privacy to support an individual's privacy of his own thoughts. What other parts of the Constitution support the privacy concerns in *Stanley, Kyllo, Safford,* and *Quon*? How might the First Amendment protection provided in *Stanley* and the Fourth Amendment discussed in the other cases expand to protect your privacy in the Internet of Things?

Reading List

1. *Stanley v. Georgia*, 394 U.S. 557, 557-568 (1969).
2. *Kyllo v. United States*, 533 U.S. 27 (2000).
3. *Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 368-381; 398-402 (2009).
4. Paul M. Secunda, *Privatizing Workplace Privacy*, 88 Notre Dame L. Rev. 277, 283-302 (2012).

Suggested Reading

1. Sonia K. Katyal, *Privacy vs. Piracy*, 7 Yale J. L. & Tech. 222 (2005).
2. Deborah Ahrens, *Schools, Cyberbullies, and the Surveillance State*, 49 Am. Crim. L. Rev. 1669 (2012).
3. Amy J. Sluszka, Esq., *Constitutional Rights of A Student: "Strip-Searched",* 6 U. Mass. Roundtable Symp. L.J. 159 (2011).

[23] Comment (a) to §7.02, Restatement (Third) Employment Law (proposed final draft April 2014).

III. Law Enforcement Data-Gathering & Decision-Making

Session 6. *Law Enforcement & the Fourth Amendment*

In the previous class session, we explored how courts usually consider a person's home to be the epitome of reasonable and thus justified privacy protection. Further, we examined how the same justifications tend to decrease privacy protections the further away from home a person is, in quasi-public places like work and school. Given this background, how do you expect courts to adapt to changing technologies both in and outside of the home?

The Fourth Amendment protects against unreasonable searches and seizures, but just what makes a search "reasonable" is the subject of much debate. Reasonableness is grounded, at least in part, in people's expectations in a given context. A central challenge in Fourth Amendment cases is to determine whether the government's law-enforcement interest outweighs a person's privacy interest in being free from unwanted government intrusion?

The Kerr reading for this week proposes a new theory to explain common principles that, he argues, run through all Fourth Amendment jurisprudence as courts try to adapt the law to changing technologies. After reading his article, see if you can spot where the Supreme Court may or may not rely on those principles in *Riley*, a case about the warrantless search of a cell phone in the context of an arrest.

Notes & Questions

Kerr

1. Does Kerr's "equilibrium" theory help you make sense of what many call the "mess" of Fourth Amendment case law as Kerr explains it? Or might there be a better way courts should interpret the Fourth Amendment as technology develops? Can you think of other areas of privacy law we have discussed in the course so far, or other areas of the law you have studied, that have an overarching theory to help courts interpret laws in light of new facts that did not exist when the laws were originally written?
2. What do you make of Kerr's claim that his normative equilibrium theory is functionally different from "common law reasoning" (p. 492-93)? Is the "Year Zero" concept something courts, legislatures, and law enforcement do, can, or should use to keep many kinds of laws in line with new technologies? In other words, to what other areas of the law might Kerr's equilibrium concept apply? For example, Kerr

argues that in the Fourth Amendment context, courts implicitly use the equilibrium theory to restore a pre-existing balance of police power. In other areas of privacy law, such as the privacy torts or data privacy, are courts not also implicitly trying to restore a preexisting balance of expectations of privacy? To the extent that the equilibrium adjustment theory is a tool, what are the arguments for limiting it to interpret Fourth Amendment only?

3. How might the equilibrium adjustment theory explain how courts could respond to forthcoming Internet of Things technology? Consider, for example, a self-driving car that connects to your alarm at home, your coffee maker at work, and other online resources that provide data about your schedule, traffic and weather conditions. This car can cull all of the data and make sure that you get up on time, that your car is running and warm if it is a cold and frosty morning, and that by the time you get to work, your coffee is made fresh when you arrive.
    a. If law enforcement wants to search any of these devices or even the data itself, how might it do so? Are these devices more or less similar to the various kinds that Kerr describes – sense enhancing devices like thermal imaging, beepers and GPS; or cars themselves; or a telephone network surveillance, which may include the contents of calls and/or the numbers dialed? (p. 496)
    b. Is surveilling data from devices about your home more like an undercover agent situation (p. 518-19)? Why or why not? Do the rules from Year Zero and the equilibrium adjustment theory help you answer?

Riley

1. Does the Supreme Court here frame the issue as Kerr predicts? Is the Court trying to adapt the new technology (smart phone and cloud storage technology generally) to Year Zero? How so?
2. Are any of Kerr's six scenarios implicated here? These include: the government uses a new tool to field evidence; criminals use a new tool to evade detection; new crimes and new practices; both criminals and the police use a new tool; the status quo; defending countermeasures (Kerr, p. 489). Does this categorization help frame the discussion of Fourth Amendment protections?
3. Does it make a difference, in the equilibrium adjustment theory or other Fourth Amendment reasoning generally, that the search in *Riley* was a warrantless search incident to arrest rather than a non-arrest search?
4. Does the *Riley* decision adequately protect individual private interests in protecting their digital data against intrusions? (See footnote 1). How do you think a court would apply the Fourth Amendment in non-arrest searches of aggregated digital information?
5. The Court outlines law enforcement's key concerns in making arrests: officer safety and evidence preservation. How might possible technologies from the Internet of Things increase or decrease risks officers face in the arrest situation? Do the easy methods that the *Riley* court mentions as available to thwart such risks from smart

phones (such as disconnecting a device from network) provide enough protection in the IoT context? The Court asserts that the availability of the exigent circumstances doctrine is adequate for more dangerous situations. Does this assertion hold true with IoT technologies?

6. The *Riley* Court further finds that "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape." (p. 10) Replace the word "cell phone" with an IoT device, either existing or that you can dream up. Can you imagine a scenario that disproves the Court's theory that data itself is never an immediate physical threat?
7. Recall the class discussion in session two about Solove's "digital biography" concept. Does the Court in *Riley* adequately address this concern?

Reading List

1. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 478, 478-508; 512-522; 533-543 (2011).
2. *Riley v. California*, 134 S. Ct. 2473, 573 U.S. _____ , *1-22, 25-28 (2014).

Suggested Reading

1. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62 (2013).
2. Patrick M. Rahill, *Top Secret-the Defense of National Security Whistleblowers: Introducing A Multi-Factor Balancing Test*, 63 Clev. St. L. Rev. 237 (2014).

Session 7. *National Security & Foreign Intelligence*

In this session, we continue to explore the evolution of law-enforcement data gathering and decision making by further examining theories of Fourth Amendment jurisprudence and by analyzing government practices in domestic and international surveillance. Recall prior readings and discussions about digital biographies, expectations of privacy, and public interest goals. How do you expect these ideas to work in the context of national security?

Notes & Questions

Shane

1. Shane describes the evolution of how the law treats and defines "trap and trace" devices and "pen registers," noting that Patriot Act broadened the definition to include collection of *content* from such devices. Was this expansion a justified response to evolving technology, particularly in light of Kerr's normative equilibrium adjustment theory we discussed in the last class?
2. What are the differences between the kinds of surveillance programs developed in presidential administrations (e.g., the Bush Administration and the Terrorist Surveillance Program) and those developed by Congress (e.g., the Foreign Intelligence Surveillance Act)?
3. Where do you see Internet of Things fitting in this landscape, given that metadata is a crucial part of the technologies' functionality? Given the background Shane provides, could metadata alone be the subject of electronic surveillance just because it is transmitted to the cloud?
4. Is the secrecy of the United States Federal Intelligence Surveillance Court justified (e.g., the ex parte proceedings)? Do you need more justification than a simple weighing of the public interest and private interest provides?
5. What role do the cooperating telephone companies play in the government's surveillance and data gathering efforts? Are these companies unjustly violating the privacy of their customers? To what standard should we hold such entities?
6. Recently, some smartphone companies have strengthened their encryption technologies because of the criticism they faced due to their cooperation with the NSA and the FBI. President Obama and leaders of other countries would like for law enforcement and intelligence agencies to have access to encrypted messages (and the data contained within such messages) through "backdoors," which are "hidden entryway[s] in a program that bypasses the regular login process." Backdoors

weaken encryption technology, making it easier for bad actors to get in.[24] Is that a good trade-off?

Etzioni

1. Compare and contrast Kerr's equilibrium-adjustment theory with Etzioni's theories. Does one provide a more applicable or realistic doctrine for emerging technologies and the privacy issues they may create, or do they work together? Etzioni references Kerr often, but are their theories really that similar?
2. Etzioni disassembles the private-public distinction as we know it, positing that there is really just a "personal sphere" and we should be concerned with "protecting personhood." (p. 12) He also describes his theory as purposefully avoiding questions about reasonable expectations of privacy in favor of looking for ways the law can comport with societal values. Are his theories really so different from what we have studied so far?
3. He calls his underlying theory of the Fourth Amendment and subsequent jurisprudence the "liberal communitarian philosophy," and explains that this way of thinking differs from "authoritarian and East Asian communitarian" and libertarian and contemporary liberals' ways of thinking. Which of these philosophies better describes how privacy from governmental intrusion should develop? Is there a better philosophy that Etzioni excludes from discussion? What factors are important in determining the overall philosophy in this area of law—do you look at what the Framers might have chosen, or what most people would reasonably expect, or what societal values are (if that is indeed a different concept from reasonable expectations)?

Reading List

1. Peter M. Shane, *The NSA and the Legal Regime for Foreign Intelligence Surveillance*, [foreward] 10 ISJLP 259 (2014).
2. Amitai Etzioni, *A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach*, 10 ISJLP 641 (2014).

Suggested Reading

1. *U.S. v. U.S. Dist. Court for Eastern Dist. of Mich.*, Southern Division, 407 U.S. 297 (1972). (The *Keith* case)
2. Dan Fenske, *All Enemies, Foreign and Domestic: Erasing the Distinction Between Foreign and Domestic Intelligence Gathering Under the Fourth Amendment*, 102 Nw. U. L. Rev. 343 (2008).
3. Attorney General Guidelines for FBI Criminal Investigations, National Security Investigations, and the Collection of Foreign Intelligence, S. Hrg. 110-846, September 23, 2008.

[24] *See generally* "Broad alliance emerges to fight Obama tech policies," John Shinal, *USAToday*, Mar. 17, 2015; and "Obama Wants Tech Companies to Install Backdoors for Government Spying," Will Oremus, *Slate.com*, Jan. 19, 2015.

IV. Public Access to Information

Session 8. *Public Access to Government Data*

What is privacy in the context of information in the public domain? Can information in the public domain (e.g., court records, public records, FOIA information) *also* be kept secret to some extent, or are these forms of publicness and privateness mutually exclusive? The reading for this class explores these themes. Before delving into the reading, consider this fundamental question: what do we want privacy law to accomplish?

You may recognize that the Solove materials for this class comprise the rest of the article which was first excerpted in the second class of this course. In reading through the materials for this session, recall the discussion and reading from that session about the aggregation of data and digital identities that can be created through such aggregating processes. Those concepts are central to the topic of this class session as well.

Lastly, please note that since the assigned Solove article was published, the Freedom of Information Act (FOIA) has been amended to preclude agencies of the "intelligence community" from disclosing records in response to any FOIA request that is made by any foreign government or international governmental organization, either directly or through a representative. This amendment is the first time that Congress has departed from the general rule that "any person" may submit a FOIA request.[25]

Notes & Questions

1. Solove conceptualizes privacy as a function of a person's expectations of a limit on the degree of accessibility of information. (p. 1141). How does this theory compare to Kerr's imagined Year Zero concept covered in the previous class session?
2. Can you think of an example of how government data-mining and analysis of such data is beneficial? Perhaps the answer depends on what point of view you take. For example, think of yourself as a prospective home buyer in Athens, Georgia. Pick an address in Athens and see what you can find out about that address by exploring its public record on the local tax assessor's website, available at http://www.qpublic.net/ga/clarke/search.html. Are you surprised by the amount or type of information available? What expectations did you have about the degree

[25] Amended by the Intelligence Authorization Act of 2003, effective as of November 27, 2002. See Pub. L. No. 107-306, 116 Stat. 2383 (2002); *see also* US Justice Department Guide to FOIA, Introduction, page 6 (2009) available at http://www.justice.gov/oip/foia_guide09/introduction.pdf.

of access someone might have to such data? What can you learn about a person from looking at these records?

3. Solove explains the inherent tension between transparency and secrecy in the accessibility of government records. What factors tip the scale in favor of one over the other? For example, does the relative weight of transparency or secrecy depend on whether one is an individual company, a government, or a consumer? Consider the advertising industry: Companies can use public records to glean information about your future behavior. You may take certain actions that indicate you are looking to move. Thereafter, you receive unsolicited mail about moving services, realtors, and the like. On the one hand, it is helpful for you to see information that is tailored to you, as you will not waste your time reading ads that are not relevant to you. You may even see an ad for something that is similar to and better than what you were originally looking for. This example is a positive one for the consumer and the advertiser; but what are the potential harms in such activities? Is there a harm in terms of the privacy torts discussed earlier in the course? (e.g., Solove discusses privacy tort cases on p. 1179-08)
4. Expectations appear to remain a key part of determining privacy, despite what scholars Kerr and Etzioni have highlighted. That said, do we really expect privacy when things are in the public domain? Should we expect all of our identifying information to be in the public domain? Consider Solove's description of how our expectations of privacy are linked to our understanding of how they are accessed (one in millions, p. 1178).
5. How practical is Solove's solution (p. 1198) to redact personal information from public records, when he also argues that aggregation of individual pieces of information is the harm? In other words, how adequately does his solution address the supposed harms related to aggregated data from public records?

Reading List

1. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1137-1184; 1895-1206 (2002).

Suggested Reading

1. Department of Justice Guide to the Freedom of Information Act (2009), available at http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/introduction.pdf (last accessed May 8, 2015).
2. Patricia M. Wald, *The Freedom of Information Act: A Short Case Study in the Perils and Paybacks of Legislating Democratic Values*, 33 Emory L.J. 649 (1984)
3. James T. O'Reilly, *Expanding the Purpose of Federal Records Access: New Private Entitlement or New Threat to Privacy?*, 50 Admin. L. Rev. 371 (1998)
4. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 585 (2014).
5. Joe Regalia, *The Common Law Right to Information*, 18 Rich. J.L. & Pub. Int. 89 (2015).

6. Sara E. Stratton, *Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media*, 41 Hastings Const. L.Q. 649 (2014).

V. Private Industry Data-Gathering and Decision-Making

Session 9. *Consumer Privacy*

Consumers and companies rely heavily on various forms of credit in their transactions, from purchasing a car to buying clothes to renting an apartment.[26] Credit reporting agencies "prepare credit reports about people's credit history for use by creditors seeking to loan people money."[27] These reports can contain basic financial information about an individual (such as bankruptcy filings or mortgage foreclosures), and some companies supplement these basic reports with "information about an individual's character and lifestyle."[28] The combination of the types of personal information within the reports, along with how they are used in the marketplace, creates opportunities for misuse and invasions of consumer privacy. In this session, we explore the Fair Credit Reporting Act and enforcement practices of the Federal Trade Commission.

Before you read the materials, think about the following questions: What are your expectations of privacy as a consumer, generally? Do they change when you are on line versus when you are purchasing something in person? What are your privacy expectations for data about your transaction history and your purchasing habits? How can you, or do you think you need to, control the dissemination of this kind of information?

Notes & Questions

Smith v. Bob Smith Chevrolet

1. Have you made a car purchase like the one in *Smith v. Bob Smith Chevrolet*? If so, do you know whether the car seller accessed your credit score and how it used the score? What makes this kind of access different from Bob Smith Chevrolet's access of the plaintiff's credit report in February 2000? Why does the court say that one kind of access is acceptable but the other is not, considering that the same information is disclosed in both reports?
2. The court says that Bob Smith Chevrolet may access the plaintiff's credit report only if its actions are consistent with the permissible purposes in 15 U.S.C. § 1681b(a)(3). (p. 815). Then, the court states that all of these permissible purposes have two goals: "to provide a benefit to a consumer or to collect a pre-existing debt." (p. 817).

[26] Solove & Schwartz, *Privacy, Information, and Technology*, 3rd Ed. (2011), at 383 2011.
[27] Id.
[28] Id.

Do these goals accurately interpret what Congress intended, or do you think the permissible uses cover more core goals? What role does the Federal Trade Commission and its interpretation of the Fair Credit Reporting Act have in the court's reasoning?

3. The court establishes a rule regarding the intent of the credit report user in the context of accessing a credit report. The intent should be based on an existing belief rather than on a "belief that the original transaction was mistaken." (p. 820) Do you see any potential problems with the future application of this rule? Why is this scenario so different from the "bad check" situation that the court argues is distinguishable in Footnote 3?
4. In the last part of the opinion, the court discusses the invasion of privacy claim and finds that the evidence does not support granting the plaintiff's motion for summary judgment. What do you think would help establish the invasion of privacy tort in this case? Should any factors of the tort change in the context of accessing credit reports?

Serwin

1. Serwin asserts that "one cannot fully exercise the right to be let alone unless there is notice – an understanding of the potential occurrence—of the potential privacy invasion, and you have the opportunity to choose to be let alone – freedom to determine when and where one's information is disclosed or used." (p. 818). What do you think of this comparison of Warren and Brandeis' article to the FTC's "notice and choice" model of consumer privacy protection and enforcement (i.e., "Privacy 1.0.")?
2. The Federal Trade Commission and others propose models of privacy to address most privacy interests, including "models based upon accountability," use-limitations, and Serwin's own "Privacy 3.0" that is based on proportionality. (p. 812, 844-852). What is different about these models of privacy in the consumer context versus the government surveillance context? Imagine that every January 1st you get a notice in the mail that has language similar to privacy policies you see from companies, except this notice comes from the government and explains what its policy for reasonable searches will be for the coming year. Why might you find this kind of notice unacceptable coming from the government, but you routinely accept it from businesses? What different privacy interests are at stake?
3. Find and examine a privacy policy that you have seen recently, such as one from a recent app you downloaded or a website you visited. Of the kinds of models Serwin describes, what kind is that privacy policy emulating? Does it adequately address the typical three main elements of privacy laws (p. 844):

    (1) Classify or identify data that is to be regulated

(2) Regulate the processing of data through conduct limitations, including the level of consent required to collect or use the data, data security limitations, use restrictions, and other limitations; and
(3) Provide for enforcement for violation of point (2).

What other places, besides privacy policies you agree to in everyday transactions, do you expect to see the implementation of some of the solutions that the FTC proposed or that Serwin proposes in this 2011 article, such as the FTC's "privacy-by-design" framework (p. 812) or Serwin's Privacy 3.0 model of proportionality (p. 849-852)?

Reading List

1. *Smith v. Bob Smith Chevrolet, Inc.*, 275 F. Supp. 2d 808, 808-813; 815-822 (W.D. Ky. 2003).
2. Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 San Diego L. Rev. 809 (2011).

Suggested Reading

1. "Consumer Privacy Bill of Rights," White House, Feb. 23, 2012 available at https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (last accessed May 8, 2015).
2. Christin S. McMeley, *Protecting Consumer Privacy and Information in the Age of the Internet of Things*, 29-FALL Antitrust 71 (2014).

Session 10. *Medical Privacy*

Recall the discussions in the third session of this course where you examined specific provisions and federal agency guidance about the Health Insurance Portability and Accountability Act (HIPAA). There, we analyzed HIPAA provisions not only as an exercise in applying the law to real-world scenarios but also as a way to appreciate the challenges legislatures face when adapting law to changes in technology and privacy expectations. Keep those previous readings and discussions in mind as you read the materials for this session. Here, we explore relevant legislation and regulations along with practical implementation issues that arise given technological advancement in the health information technology and security spheres. What problems do new technologies, such as Internet of Things devices, pose for individuals, healthcare providers, and regulators? What can and should legislatures, courts, and health data aggregators do to protect patients' privacy interests?

Notes & Questions

Gantt

1. What kinds of policy approaches, including those discussed by Swire, might help address the hacking threat that healthcare systems invite? As Gantt explains, HIPAA addresses the privacy and security of patient health information (PHI) (p. 235), but the Department of Homeland Security also finds that health care systems are an "inviting target to activist hackers, cyber warriors, criminals, and terrorists." (p. 239). What institution or set of institutions are in the best position to prevent the harm that occurred in Gantt's opening factual scenario?
2. Gantt draws an analogy between the banking industry and the healthcare industry (p. 247) in order to generate potential security standards for ePHI. Are Gantt's proposed modifications feasible? (p. 253-258). Is the finance-healthcare comparison even a workable analogy? What other industries or security practices might provide guidance in creating effective security standards for health data?

Swire

1. Swire argues that no other institutional approach besides the regulations of HIPAA Privacy and Security Rules would have achieved the goal of creating national health privacy standards, particularly in light of the "overall shift to electronic billing records in health care." (p. 657, 658). Do you agree? What role might the public, including patients and doctors, have played in achieving this goal, given that

"medical data is widely understood to be especially sensitive, and the idea of medical confidentiality is even included in the Hippocratic Oath"? (p. 656).

2. As Swire notes, "HIPAA notices have become a ritual when you see a new doctor but do not do much to actually inform patients about their choices." (p. 656). In your own healthcare experiences, what do you recall about HIPAA notices? Have you ever encountered Electronic Health Records (EHRs), or do you know whether your health care providers have used them? Should it be an option for patients to opt-out of EHR programs, for instance in the case of someone wanting to be in full control of their digital identity, including health information?
3. Swire discusses HIPAA, EHRs, internet privacy, and cybersecurity in separate sections and does not appear to examine possible connections among these issues. Take his paper to this next step. In other words, health information technology inevitably intersects with internet and cybersecurity concerns, especially with the advent of mobile technology and Internet of Things devices; so, how might you synthesize Swire's "imperfect alternatives" analyses? Is there a single policy approach or a combination of policy approaches that might address the convergence of these related concerns?
    a. For example, in his discussion about internet privacy in Section IV, Swire states that privacy on the internet faces both market and government failures, but that the approach of self-regulation with credible threat of government intervention has worked. (p. 663) How might this approach apply to health data (which Gantt considers in a separate section), given the utilization of EHRs and the advancement of IoT devices?

Reading List

1. Gordon Gantt, Jr., *Hacking Health Care: Authentication Security in the Age Of Meaningful Use*, (Note) 27 J.L. & Health 232 (2014).
2. Peter Swire, *Finding the Best of the Imperfect Alternatives for Privacy, Health IT, and Cybersecurity*, 2013 Wis. L. Rev. 649 (2013).

Suggested Reading

1. Michael L. Tudor, *Protecting Privacy of Medical Records of Employees and Job Applicants in the Digital Era Under the Americans with Disabilities Act*, 40 N. Ky. L. Rev. 635 (2013).

Session 11. *Data Security & Identity Theft*

As we have discussed throughout the course, despite the many benefits consumers, companies, and government entities can attain from the collection and aggregation of massive amounts of data, these benefits are not without significant privacy risks. In this session, we will consider the dangers that organizations "of all sizes and across all industries face," including "[c]yber theft, cyber extortion, mobile device loss, misappropriation of confidential business information, and unauthorized disclosures of protected information."[29] In creating their data security protocols, organizations must not only consider these potential harms, but they must also comply with various laws, regulations, and industry standards. Like its regulation of privacy law generally, the United States uses a piecemeal system of federal and state laws along with common law principles to regulate the "collection, use, processing, disclosure, and security of personal information," rather than a single, comprehensive federal law.[30] An organization that fails to comply with all of the relevant privacy and data security laws may suffer substantial consequences including:

- Government-imposed civil and criminal sanctions, including fines and penalties.
- Significant fines and damages awards resulting from private lawsuits, including class actions (permitted under some privacy and data security laws).
- Damage to the company's reputation and customers' confidence and trust, resulting in lost sales, market share and brand and stockholder value.[31]

As we discuss the structural security challenges that organizations face due to potential harms and the lack of comprehensive federal guidance, it is important to keep in mind an underlying harm that individuals are at risk of encountering if organizations fail to adequately protect their personal information—identity theft. Is this harm sufficiently protected against in the current legal regime or with Sloan's proposed security framework?

---

[29] Peter Sloan, The Reasonable Information Security Program, 21 Rich. J.L. & Tech. 1, 1 (2014), available at http://jolt.richmond.edu/v21i1/article2.pdf.
[30] "US Privacy and Data Security Law: Overview," *Practical Law* Practice Note 6-501-4555 (maintained).
[31] Id.

Lastly, consider what might make data security fundamentally different from data privacy. While the term "data privacy and security" broadly relates to "everything relative to data gathering, storing, destroying, and sharing,"[32] differentiating the two may help frame the discussion for this session. For instance, privacy is a kind of fundamental right,[33] whereas security is a set of protocols that ensure privacy of data, meaning "people who are not authorized to see private data cannot examine it."[34] In other words, data security is a means to an end of data privacy. How do you think a right to privacy drives privacy and security policies?

Notes & Questions

1. Consider the premise that Sloan uses to set up his article:
   > "[I]nformation security laws share a common theme of reasonableness. The notion of reasonableness permeates explicit statutory and regulatory requirements for safeguarding information, and appears to be a central tenet of FTC enforcement orders regarding information security. Yet such legal requirements and orders frequently fail to specify what reasonableness means in their particular domains. And so, one is left to wonder, what constitutes a "reasonable" information security program?" (p. 2)

   Recall the various laws, regulations, and guidelines developed by government agencies we have studied in this course; do you agree with this basic premise? Are there some privacy laws or regulations that rely more on reasonableness than others? What other common themes can you identify in the laws and regulations we have studied? For example, does the expectation of privacy play a role in most privacy-related laws? How might the expectation of privacy and reasonableness be connected in the data security arena, or are they separate concepts altogether?
2. Sloan gleans and identifies four factors from most information security laws (p. 26-27), and then he proposes a set of six elements for a reasonable security program:
   (1) Identify: An organization should identify the types of information in its possession, custody, or control for which it will establish security safeguards ("Protected Information");

[32] Steven A. Meyerowitz, *Interview: Rania V. Sedhom Discusses Global Data Privacy And Security Issues*, Pratt's Privacy & Data Security L. 2010.02-12.
[33] Id. *But see generally* Kenneth Einar Himma, *Privacy Versus Security: Why Privacy Is Not an Absolute Value or Right*, 44 San Diego L. Rev. 857 (2007) (noting that the scope and protectability of privacy rights is part of an ongoing debate).
[34] Meyerowitz.

(2) Assess: An organization should assess anticipated threats, vulnerabilities, and risks to the security of protected information;
(3) Safeguard: An organization should establish and maintain appropriate policies and administrative, physical, and technical controls to address the identified threats, vulnerabilities, and risks to the security of protected information;
(4) Contract: An organization should address the security of protected information in its third-party relationships;
(5) Respond: An organization should respond to detected breaches of the security of protected information; and
(6) Adjust: An organization should periodically review and update its policies and controls for the security of protected information.

Compare these six elements with the four legislative factors. What does Sloan prioritize? Recall Andrew Sewrin's article we discussed in session 9, where Serwin proposes a privacy regulatory model where "[u]se limitations should be proportional to the sensitivity of data," and the sensitivity of data would have four tiers—"highly sensitive, sensitive, slightly sensitive, and nonsenstive."[35] Is Sloan indifferent to the sensitivity of data, or what the information being protected is about? If so, how would you modify his security policy recommendations to take this issue into account? In other words, is the reasonableness concept along with the six elements an effective way to think about the problem of data security, or should we think more critically about the type of data being secured?

3. How do trade secret processes influence or relate to data security protocols? What are the kinds of harms that each set of procedures tries to prevent? Besides trade secret law, what other areas of the law might address similar harms as those that threaten data privacy, and how would they help influence data security law and policies?

Reading List

1. Peter Sloan, The Reasonable Information Security Program, 21 Rich. J.L. & Tech. 1, 25-92 (2014), available at http://jolt.richmond.edu/v21i1/article2.pdf.
    a. Section to read: III

Suggested Reading

1. Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 Me. L. Rev. 373 (2014).
2. Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 Ariz. L. Rev. 1171 (2014).

[35] Andrew Serwin, The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, 48 San Diego L. Rev. 809, 850 (2011).

3. John L. Jacobus, *Benjamin B. Watson, Clapper v. Amnesty International and Data Privacy Litigation: Is A Change to the Law "Certainly Impending"?*, 21 Rich. J.L. & Tech. 3 (2014).

VI. International Perspectives

Session 12. *Privacy & Globalization, International Laws, & Cultural Differences*

This course has focused primarily on federal and state laws from the United States, but privacy is truly a global issue, and a course about privacy like this one will not be complete without a comparative law component. In this session, we will focus on comparing the United States and the European Union, starting with a brief introduction to the different conceptions of privacy that have developed in the United States and England since the 19th century. Despite the discrepancy in how these two countries developed their privacy regulations, there are some signs that the approach to privacy regulation is actually converging among many different countries around the world.[36] For instance, the Fair Information Practice Principles (FIPPs), created by a U.S. agency in 1973 "form the backbone of many EU privacy laws, as well as the OECD Privacy Guidelines, which form the backbone of many privacy laws around the globe." Because of the great influence that the EU and U.S. have rest of the world, this session will focus primarily on privacy law from those two regions.

Notes & Questions

1. The conceptual and doctrinal differences that Richards and Solove discuss in their article relate to the development of privacy tort law (the breach of confidence tort in England, and the myriad of U.S. privacy torts, including public disclosure of private facts). How does their explanation about the development of privacy torts relate to Schwartz and Solove's explanation about the U.S. and EU's underlying philosophies in defining personal information? Is the U.S.' focus on individual privacy represented in its privacy law concern of "redressing consumer harm and balancing privacy with efficient commercial transactions;" and is England's focus on relationships represented in the EU's view of privacy as a "fundamental right that can trump other interests"? (Schwartz & Solove, p. 877). Should the development of English privacy law even be considered in the context of EU privacy laws? If not, what kind of historical background would be more appropriate?

[36] *See generally*, Daniel J. Solove & Neil Richards, Privacy Law: From a National Dish to a Global Stew, Technology | Academics | Policy (TAP), (Apr. 14, 2015), http://www.techpolicy.com/Solove-Richards_PrivacyLaw-FromNationalDishToGlobalStew.aspx ("New countries keep recognizing the Warren and Brandeis torts. And countries are also adopting EU-style privacy laws. US-style data breach notification laws are increasingly popular – the EU has been hungrily eying US breach notification laws, eager to cook up some of their own.").

2. In the United States, "personal information" is not defined in a "coherent and consistent manner," as there is no one, all-encompassing U.S. privacy regulation; (Schwartz & Solove, p. 887) rather, there is a mix of state and federal laws. However, even given that federalism is a core political concept in the United States, does it make sense for states to have any say in defining "personal information," particularly when the flow of data is not limited by the borders of states, and where privacy is such an international issue? Should Congress be in charge of creating a comprehensive privacy regime, or does its track record for inconsistent and underdeveloped national privacy laws make it necessary for states to work out privacy policies on their own? How does the tradition of states being in control of tort law affect your reasoning, considering the relevance privacy tort development? How would you apply these issues to the European Union context and its 28 member countries?
3. Describe the differences between "identified" and "identifiable" data that the Schwartz and Solove describe for their PII 2.0 information continuum. (p. 905-908). Should regulators try to push Internet of Things companies to prefer one over the other?

Reading List

1. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L. J. 123, 173-178 (2007).
    a. Sections to read: III. C. 1 & 2
2. Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877 (2014).

Suggested Reading

1. McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 Geo. Wash. Int'l L. Rev. 643 (2012).
2. Jennifer Daskal, *The Un-Territoriality of Data*, forthcoming Yale Law Journal 2015/2016, available at http://ssrn.com/abstract=2578229.

VII. Conclusions

Session 13. *First Amendment Limitations on Data Privacy*

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*
>
> First Amendment, U.S. Constitution

How might the constitutional right of free speech limit data privacy regulation? Consider the nature of data itself. How is it similar to or different from more familiar forms of expression or "speech" that come under the purview of the First Amendment? Does your answer depend on how you define "data" and "speech"? The materials for this session appear to present two opposing sides to a debate on the issue of whether or not the First Amendment is implicated in data privacy laws. To help determine how much the authors agree and disagree, as you read each piece, consider how the authors' arguments apply to a privacy law we have discussed. For instance, try working through their first amendment analyses using the scenario in *Smith v. Bob Smith Chevrolet*,[37] which we discussed in the ninth session, where a car salesman improperly accessed a purchaser's credit report, violating the Fair Credit Reporting Act.

Notes & Questions

1. The two authors here may seem at first glance to be at opposite ends of a debate – just look at the opening lines in the abstracts of their articles:
    - Bambauer: "Privacy laws rely on the unexamined assumption that the collection of data is not speech. That assumption is incorrect."
    - Richards: "Laws regulating the collection, use, and disclosure of personal data are (mostly) constitutional, and critics who suggest otherwise are wrong."

    Plus, Richards claims he "want[s] to show why asking 'is data speech?' is a poor way to ask a very important question." (p. 1523). However, despite the title, the main question Bambauer seeks to answer in her article "Is Data Speech?" is "whether regulations on the collection or transfer of data implicate the First Amendment, thus

[37] 275 F. Supp. 2d 808 (W.D. Ky. 2003).

requiring the government to justify and narrowly tailor the regulations." (p. 66). Does Richards' article have a substantially different purpose? What are the key differences in how these two authors approach the issue of first amendment limits on data regulation?

2. These two authors appear to be talking across from each other. Try to find ways of connecting the two. What concepts might they agree on, even if on a very general level?
    a. For instance, Bambauer finds the disparate treatment of the dissemination of data and the creation of data to be a crucial mistake in First Amendment jurisprudence. Richards does not address this point. He finds that regulation of commercial data flows based on FIPs is constitutional given the development of constitutional and regulatory law since the New Deal. Bambauer does not address this point in her article. How might each author respond to the other's reasoning?

Reading List

1. Jane Bambauer, *Is Data Speech?*, 66 Stan. L. Rev. 57, 58-84; 91-110 (2014).
    a. Parts to read: I; II; III (B), (C)
2. Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 Wm. & Mary L. Rev. 1501, 1504-1529 (2015).
    a. Parts to read: I – IV.

Suggested Reading

1. Anupam Chander & Uyên P. Lê, *Free Speech*, 100 Iowa L. Rev. 501 (2015).
2. Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 Nw. U. L. Rev. 795 (2013).
3. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. Rev. 1149 (2005).
4. Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. Rev. 1315 (2009)

Session 14. *The Future of Privacy in a World with the Internet of Things*

Throughout the course, we have learned about privacy law and how it might apply to Internet of Things technologies. In this session, you will incorporate previous discussions and articulate how you think the Internet of Things will shape privacy law. While "Internet of Things" may certainly be considered just another internet fad, the rapid development, economic impact, and infinite application possibilities of interconnected devices cannot be denied.[38] As you reflect on past discussions and read the materials for this session, consider the parties who might be most impacted by this wave of technology.

Notes & Questions

1. Do you think people who create new IoT technologies should seek the blessing of public officials before or during development? Conversely, as laws and regulations develop to address new problems arising from IoT devices, how should legislators and regulators rely upon IoT creators when developing laws and regulations? What other industries have a strong government-business dynamic? Given that there may be substantial overlap between the creators of IoT and existing industries with a government relationship (financial, insurance, healthcare), what is the risk of capture for IoT development?
2. Thierer proposes a variety of "constructive solutions" to support the somewhat extreme "permissible innovation" method of regulation. His solutions include: digital literacy, self-regulation and privacy by design, empowerment, common-law and evolving liability standards, FTC oversight, social norms, and law enforcement. How achievable and effective are these solutions? Will the best solution depend on the type of IoT device at issue, or will all IoT devices tend to face the same privacy issues?

[38] IBM is spending $3 billion on IoT over the next four years, making a new business unit just for IoT. *See* Hayley Tsukayama, *IBM's making a new business unit just for the Internet of Things*, The Washington Post, (Mar. 31, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/31/ibms-making-a-new-business-unit-just-for-the-internet-of-things/; and Congress has a committee specifically for IoT. *See* David Kravets, *Internet of Things: There's now a US congressional committee for that*, Ars Technica (Jan. 13, 2015), http://arstechnica.com/tech-policy/2015/01/internet-of-things-theres-now-a-us-congressional-committee-for-that/.

Reading List

1. Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 Rich. J.L. & Tech. 6, 37-57; 60-74; 78-88; 98-106; 111-118 (2015), http://jolt.richmond.edu/v21i2/article6.pdf.
   a. Parts to read: III; IV(A), (C), (D), (E); V; VI. (A), (C), (D), (F), (G); VII

Suggested Reading

1. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014).
2. Omer Tene, Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 Yale J. L. & Tech. 59 (2014).