American Bar Association

What's In Store

What's In Store

Newsletter of the Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee

Volume 23, No. 1, August 2016

Editors

Svetlana S. Gans
Federal Trade Commission
sgans@ftc.gov

Lydia Parnes
Wilson Sonsini Goodrich & Rosati
lparnes@wsgr.com

Terri J. Seligman
Frankfurt Kurnit Klein & Selz PC
tseligman@fkks.com

Patricia A. Conners
Office of the Attorney General of Florida
Trish.Conners@myfloridalegal.com

M. Sean Royall
Gibson, Dunn & Crutcher LLP
sroyall@gibsondunn.com

Ashley Rogers
Gibson, Dunn & Crutcher LLP
arogers@gibsondunn.com

Shahin Rothermel
Venable LLP
sorothermel@venable.com

What's In Store is published periodically by the American Bar Association Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee.

The views expressed in *What's In Store* are the authors' only and not necessarily those of the American Bar Association Section of Antitrust Law's Consumer Protection Committee, Privacy and Information Security Committee, and Advertising Disputes and Litigation Committee. If you wish to comment on the contents of *What's In Store*, please write to:

The American Bar Association
Section of Antitrust Law
321 North Clark Street
Chicago, IL 60654.

From the Editors

Welcome to a special edition of What's In Store devoted to emerging issues of concern and interest to the next generation of consumer-protection scholars and practitioners.

Our first article is an interview with Lesley Fair, a Senior Attorney with the Federal Trade Commission's ("FTC") Bureau of Consumer Protection. Ms. Fair spent almost 20 years as a litigator with the FTC's Division of Advertising Practices and now specializes in education and compliance as the agency's business blogger. Her incisive blog and wit are legendary, and Ms. Fair discusses changes she has seen at the FTC and in consumer protection law over the past 30 years; shares why she enjoys practicing consumer protection law, including reflections on her most exciting case; and offers astute advice to law students hoping to get involved in consumer protection law.

As we noted in our last newsletter, we have been working hard on developing member-added benefits, and we are pleased to include in this edition three articles authored respectively by a recent graduate and two law students, as a part of an initiative geared toward getting young lawyers and law students interested in the consumer protection and privacy fields. The first is an article by Alex B. Lipton, who graduated from New York University School of Law in 2016. Mr. Lipton examines the contract-based and statutory "protections" that are at least arguably available to purchasers of "communications-capturing technologies" like Amazon Echo, Samsung's SmartTV, and Mattel's Hello Barbie, and explains why those protections may not be available to nonpurchaser, or "secondary," users of such products. Mr. Lipton argues that we should be should be troubled by the rise of such technologies and how they affect secondary users, and offers recommendations for the kind of legal protection that should be available to all users of communications-capturing technologies.

We also include an article by Andrew Stanley, a current student at the University of Iowa College of Law, that concerns the rise of "Big Data" and the role that "data brokers" play in tracking and selling consumers' information. Mr. Stanley describes the legal framework governing data brokers, argues that there is a lack of transparency, oversight, and legal guidelines necessary to protect consumers who may be unaware of how their data is collected and sold, and advocates for the adoption of a federal consumer protection law in this space.

Finally, we include an article by JD Moore, a current student at Pennsylvania State University—Dickinson Law, that examines the proliferation of the "Internet of Things." Mr. Moore argues that the "Internet of Things" presents multiple privacy concerns and that the current legal framework for consumer privacy is inadequate to cope with such issues. He examines the risk of consumers being specifically identified through data collection and the security of consumers' devices, as well as the regulatory activity that has occurred in those spaces, ultimately concluding that more regulation may be necessary.

As always, we welcome your feedback, and we encourage you to contact any of the editors to get more involved.

IN THIS ISSUE

Q&A with Lesley Fair, Senior Attorney with the Federal Trade Commission's Bureau of Consumer Protection

Lesley Fair is a Senior Attorney with the Federal Trade Commission's ("FTC") Bureau of Consumer Protection, where she has represented the Commission in numerous investigations of deceptive and unfair trade practices, including false advertising and fraud. She spent almost two decades as a litigator with the FTC's Division of Advertising Practices and now specializes in education and compliance as the agency's business blogger (at business.ftc.gov). In 2015, Ms. Fair received the FTC's Robert Pitofsky Lifetime Achievement Award.

In addition to writing a monthly column in Electronic Retailer *magazine, Ms. Fair is the author of* FTC Regulation of Advertising *in Food and Drug Law and Regulation (3d ed. 2015) and* The FTC & Social Media *in Social Media and FDA: The Essential Guide (2010). From 2000 to 2015, Ms. Fair served as Vice-Chair of the American Bar Association's Consumer Protection Committee.*

On the faculty of the Catholic University School of Law since 1984, Ms. Fair holds the title of Distinguished Lecturer and has twice been named Outstanding Adjunct Professor. She also teaches Consumer Protection Law at The George Washington University Law School.

1. *You've worked at the FTC for almost 30 years. What's the biggest change the FTC has undergone during that time?*

From my perspective, the scope of the Bureau of Consumer Protection's ("BCP") beat. It seemed like BCP had a lot to cover in 1987 when our job was to challenge deceptive or unfair practices on TV and in print. Add internet commerce and mobile marketing—with a staff about the same size it was in 1987— and much more is expected of every employee.

2. *How has consumer protection law changed during your time at the FTC?*

The beauty of Section 5 of the FTC Act is that those 23 words remain unchanged: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." Even as marketing methods evolve, Section 5 serves as a lodestar.

3. *What is the most exciting case you have worked on at the FTC and why?*

I've worked on a lot of interesting cases—for example, tobacco investigations that touched on the commercial speech doctrine, early infomercial cases, and one of the FTC's first internet advertising complaints. But one case stands out simply because it reminds me why I work at the FTC. The FTC sued a global company that sold water filters glued together with a chemical the EPA and World Health Organization classified as a probable human carcinogen. We interviewed dozens of consumers and defended their depositions, often around their kitchen tables. According to the pleadings, it was an "unfair or deceptive act or practice." But to them, it was a betrayal of trust. For years, one of our witnesses sent me a card around the holidays and always signed it the same way—"Have a Merry Christmas, but I just saw another false ad on TV. So get back to work." That memory is a daily reminder of why we do what we do.

4. *What advice would you give a law student who wants to get involved in consumer protection law?*

The only way to get involved is to get involved. Intern at the FTC. Work at an AG's Office through the ABA Section of Antitrust Law's Janet Steiger Fellowship Program. Enroll in a consumer law clinic. Volunteer for an ABA committee. In addition, talk to every lawyer who has the career you want, even if you have to cold-call them, and then listen to their life story. It may seem daunting at first, but here's a secret: Pretty much the only people who find lawyers interesting are other lawyers—and as a group, we're inordinately susceptible to flattery.

5. *In addition to working at the FTC, you are an adjunct professor at George Washington and Catholic University. What do you enjoy most about teaching law students?*

As lawyers, our stock in trade is persuasion—and yet a lot of law students graduate without an appreciation for the art of advocacy. (Can you imagine a med student who's never touched a body or talked to a patient?) That's why my class includes practical exercises—conducting a deposition, drafting a privacy policy, arguing a summary judgment motion. That's the pay-off for me: watching as students discover the inborn instinct for advocacy that every good lawyer has to have.

6. *If you could go back in time and give yourself advice at the beginning of your legal career, what advice would you give yourself?*

Be grateful for the job you have. That's the advice former United States District Court Judge Fred Shannon of San Antonio gave me while I was clerking for him. As a law student, I was too naïve to know I lacked the credentials for a federal clerkship. After clerking for six months, I began to review the gilt-edged resumes of next year's applicants and asked Judge Shannon why he hired me. He responded, "I knew you'd come to the office every morning thanking God you have this job." I'll never forget that. I understand the attraction of looking ahead to the next big promotion or opportunity. But for me, I'm just grateful to have a job I love, to work with dear friends who have a shared sense of mission, and to leave at the end of the day with the sense that we've done some good.

7. *Why do you enjoy practicing consumer protection law?*

I really had no choice in the matter. It's what I was destined to do. I can remember sitting in the shopping cart as a five-year-old and getting quizzed by my mother Alys Fair about whether it was a better deal to get one can of green beans for 59¢ or two for a dollar. A lot of people have forgotten that consumer protection as we know it was created not by lawyers, but by consumers—back then, usually women—demanding their rights in one of the few places where they could then wield power: the check-out counter of the grocery store. My role models were advocates like Betty Furness, Virginia Knauer, and Esther Peterson; legal giants like my former Bureau of Consumer Protection boss Jodie Bernstein; and unsung heroes like Alys Fair, who will still go toe to toe with any Meat Department Manager who dares to sell her a fatty cut of brisket.

Secondary Users and Communications-Capturing Technologies

By Alex B. Lipton, 2016 graduate of New York University School of Law [1]

Amazon Echo, a personal home assistant that responds to voice commands, captures the content of communications within your home.[2] Samsung's SmartTV records what you and others say in your

---

[1] An expanded version of this article will appear in the May 2016 edition of the New York University Law Review. *See* Alex B. Lipton, Note, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N.Y.U. L. REV. 396 (2016).

[2] *See Alexa Terms of Use*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=201809740%20 (last visited July 12, 2016) ("You control Alexa with your voice. Alexa streams audio to the cloud when you interact with Alexa. Alexa processes and retains your voice input and other information, such as your music playlists and your Alexa to-do and shopping lists, in the cloud to respond to your requests and improve our services.").

living room and transmits it to a third party.[3] Mattel's newest doll, the Hello Barbie, records what young users say to the doll and transmits that information to a server in order to improve the doll's responses to users.[4] Though they all serve beneficial purposes, these "communications-capturing technologies" record the content of user communications and transmit them back to the company or to a third party without regard to whether the recorded individual is the purchaser or a nonpurchaser user. Companies justify expansive collection and disclosure of purchaser data based on consent to privacy policies. But when did nonpurchaser users consent to having the content of their communications collected by these communications-capturing technologies? Do any legal protections exist to either prevent data collection of nonpurchaser users or protect their already-collected data?

Nonpurchaser users—whom I call "secondary users"—may use "communications-capturing technologies" such as the Amazon Echo when, for example, they visit the home of a friend. Despite secondary users' failure to consent to or even receive notice of privacy policies governing these products, their data—and, more specifically, the content of their communications—are recorded and disclosed to third parties when they use, or are simply in the vicinity of communications-capturing technologies. Moreover, due to several exceptions built into state and federal privacy statutes, secondary users cannot avail themselves of statutory protections outlined below. This article briefly surveys the protections available to product purchasers ("primary users") and explains why those contract-based and statutory protections will not be available to secondary users, leaving their privacy interests vulnerable.

I. Secondary Users Lack Contract-Based Protection

Privacy policies provide the first layer of privacy protection for primary users. Companies can add nearly any pro-seller term they choose and do not provide consumers with the opportunity to alter terms, so it might seem odd to label privacy policies as a form of privacy protection.[5] Moreover, very few users read privacy policies, which are long and difficult to understand, thus reducing their efficacy as a form of notice on the front-end of the consumer transaction.[6]

---

3 *See Samsung Privacy Policy—SmartTV Supplement*, SAMSUNG, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited July 12, 2016) ("[I]nteractive voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service provider (currently, Nuance Communications, Inc.) that converts your interactive voice commands to text and to the extent necessary to provide the Voice Recognition features to you.").

4 *See* Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, WASH. POST (Mar. 11, 2015), http://www.washingtonpost.com/ blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hellobarbie-from-hitting-shelves ("Hello Barbie works by recording a child's voice with an embedded microphone that is triggered by pressing a button on the doll. As the doll 'listens,' audio recordings travel over the Web to a server . . . . That information is used to help form Hello Barbie's responses.").

5 *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 83 (Jack M. Balkin & Beth Simone Noveck, 2004) ("Most privacy policies provide no way for customers to prevent changes in the policy. . . .").

6 *See* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014) ("Consumers seldom read the form contracts that firms offer."); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts*, 43 J. LEGAL STUD. 1, 19, 22 (2014) (providing empirical evidence in support of the argument that consumers seldom read end-user license agreements, and finding that only six per every 1000 retail shoppers read the agreements).

However, at least in principle, privacy policies provide some limited front-end and back-end protections for primary users. For example, once primary users receive notice of a privacy policy's terms, they can choose to exit the commercial relationship or continue if they do not object to the terms. This "notice-and-choice" mechanism provides primary users with a limited form of front-end privacy protection (although it relies on primary users actually reading privacy policies and choosing not to purchase or continue using the products). Though many users choose not to read applicable privacy policies, improved notice mechanisms can potentially improve the strength of this front-end protection.[7]

If a seller violates its product's privacy policy by using data inconsistent with the policy's terms, buyers can bring a breach of contract claim, thereby providing buyers with a back-end protection.[8] In practice, however, these back-end, contract-based claims rarely succeed, often because the buyer-plaintiff fails to demonstrate any damages resulting from breach.[9] Though private actions for breach of privacy policies generally do not fare well, the Federal Trade Commission ("FTC") can also bring an enforcement action when a seller breaches its privacy policy based on the FTC's broad authority to police "deceptive" trade practices.[10] Such FTC actions provide primary users with another form of back-end protection based on breach of the privacy policy.

Yet even the limited protections of privacy policies mentioned above are unavailable to secondary users. Secondary users have no ex ante opportunity to read privacy policies in any meaningful sense, obviating any protections that a notice-and-choice mechanism would provide. Similarly, secondary users are not parties to the contract formed by privacy policies, and thus cannot sue sellers for breach ex post or rely on deceptive representations in privacy policies.

Thus secondary users are unable to enjoy even the limited legal protections provided by privacy policies. Instead, secondary users must turn to and attempt to enforce a patchwork of privacy statutes not designed with communications-capturing technologies in mind. However, as discussed below, due to several exceptions built into such state and federal privacy statutes, secondary users likely cannot avail themselves of any of these statutory protections.

II. Secondary Users Lack Statutory Protection

Secondary users lack statutory protection from communications-capturing technologies. Although potential state protection has been sought in state recording statutes, which generally prohibit the interception of wire, oral, or electronic communication without consent, they have limited coverage. State recording statutes can be separated into "single-party consent" and "all-party consent"

---

7 *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027, 1036–37 (2012) (providing examples of "'visceral' notice," such as the sound of a camera shutter even with new technologies that do not have a physical shutter mechanism, that help individuals recognize potential privacy-violating activities without textual notice).

8 *See, e.g.*, *In* re Google, Inc. Privacy Policy Litig., 58 F. Supp. 3d 968, 986 (N.D. Cal. 2014) (holding that the plaintiff class adequately stated a claim for breach of contract when Google disclosed user data to third parties in violation of the company's privacy policy).

9 *See, e.g.*, *In re JetBlue Airways Corp. Privacy Litig.*, 379 F.Supp.2d 299, 324–27 (E.D.N.Y. 2005) (denying breach of contract claims under the privacy policy where plaintiffs were unable to prove damages).

10 *See, e.g.*, Complaint at 3, *In re* Nomi Technologies, Inc., No. 132-3251 (F.T.C. Apr. 23, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150423nomicmpt.pdf.

statutes.[11] Single-party consent statutes require only one party to a communication to consent to the recording in order to make the interception lawful.[12] To the extent that courts in these single-party consent states view communications-capturing technology sellers as a party to the communication who consented to the interception of secondary user communications, the interceptions will be deemed lawful, and thus secondary users in these states have no legal recourse under such statutes.

In states with all-party consent statutes, where all parties to a recording must consent in order to make an interception lawful, sellers must argue either that secondary users consented to the interception of their communications, or that a different statutory exception applies. For communications-capturing technologies that require the push of a button or a voice command before recording, sellers can argue that secondary users consented to the interception of their communications when performing these actions.[13] For example, the Hello Barbie requires the push of a button on the doll before recording any communications, suggesting that the user at a minimum acknowledges that recording takes place upon the push of the button. All-party consent statutes only require consent to the *interception* of communications, not consent to all of the terms provided in the product's privacy policy. Sellers may argue that secondary users who push a button or activate the product through a voice command consented to the *interception* of their communications, even if they did not consent to all of the terms present in the privacy policies, thus making even the protections under all-party consent statutes unavailable. Alternatively, if this consent argument fails, many state recording statutes authorize the interception of communications where recording is a necessary incident to the rendition of service.[14] In the communications-capturing technology context, sellers could argue that intercepting secondary user communications is both incidental and necessary to the provision of consumer products which feature speech- and voice-recognition technology.[15] This exception would remove state statutory protections from secondary users even if courts recognize that secondary users never consented to the recording of their communications.

---

11 *See* Reporters Comm. for Freedom of the Press, REPORTER'S RECORDING GUIDE 2 (2012), http://www.rcfp.org/rcfp/orders/docs/RECORDING.pdf (providing an overview of state and federal recording statutes).

12 *See, e.g.*, DEL. CODE ANN. tit. 11 § 2402(c)(4) (2015).

13 *Cf.* RESTATEMENT (SECOND) OF CONTRACTS § 19 cmt. a (1981) ("Words are not the only medium of expression. Conduct may often convey as clearly as words a promise or an assent to a proposed promise."). Though button-pushing or voice commands may constitute assent under the Restatement, in a recent case, even Chief Justice Roberts and Justice Scalia acknowledged that users may be confused about the ramifications of pushing a button with new technologies. During oral arguments in *City of Ontario v. Quon*, 1560 U.S. 746 (2010), Chief Justice Roberts admitted confusion surrounding the routing of text messages through service providers, saying "I thought, you know, you push a button; it goes right to the other [cell phone]." Transcript of Oral Argument at 49, *City of Ontario v. Quon*, 560 U.S. 746 (2010) (No. 08-1332). Justice Scalia responded, saying "[y]ou mean it doesn't go right to the other thing?" *Id.* The open question is not whether users reasonably expect they are being recorded when they use communications-capturing technologies, as recording is inextricably linked with the voice-recognition service these products provide, but whether users reasonably expect that their recordings are being transmitted to a third party or other centralized source.

14 *See, e.g.*, FLA. STAT. ANN. § 934.03(2)(a)(1) (West 2001 & Supp. 2015).

15 Several privacy policies of communications-capturing technologies include language recognizing that incidental communications capture will be a necessary incident to providing voice recognition services. *See, e.g.*, *Samsung Privacy Policy—SmartTV Supplement*, SAMSUNG, http://www.samsung.com/sg/info/privacy/smarttv.html (last visited Jan. 11, 2016) ("To provide you the Voice Recognition feature, some interactive voice commands may be transmitted (along with information about your device, including device identifiers) . . . to the extent necessary to provide the Voice Recognition features to you.").

Federal protection under the Electronic Communications Privacy Act ("ECPA") also evades secondary user communications due to two statutory exceptions. ECPA generally prohibits the interception of wire, oral, or electronic communication without consent of either the "originator" or the "intended recipient."[16] Much like single-party consent statutes, no violation occurs when the intended recipient (i.e. one party to the recording) consents to the disclosure of communications to a third party. Sellers will therefore argue that they were the intended recipient of communications intercepted by the communications-capturing technology and that only their consent was required to avoid violations under ECPA. As long as courts accept the argument that communications-capturing technology sellers are the intended recipients of these communications, secondary users would not be able to make claims against the seller under ECPA.[17]

The second relevant exception under ECPA allows providers to divulge the contents of a communication "as may be necessarily incident to the rendition of the service . . . ."[18] Communications-capturing technology producers could argue that secondary user data collection is "necessarily incident" to the rendition of both voice-recognition and personalization services provided by the company. If this argument succeeds, then secondary users would not be able to bring suit against communications-capturing technology producers under ECPA.

III. Designing Protections for Secondary Users

In designing protections for secondary users, back-end protection is superior to front-end protection in the form of notice via a privacy policy. Requiring front-end notice would impose unreasonable friction in the user experience without providing any meaningful benefit to secondary users. Consider, for example, the Hello Barbie product described above.[19] If Mattel authenticates the primary user through voice recognition—a simple process already used in high-security financial settings—it could then distinguish between primary users and secondary users and provide secondary users with notice and an opportunity to consent to the privacy policy before using the product. However, because the Hello Barbie and similar communications-capturing technologies do not have a visual display, the secondary user has no simple means of viewing the privacy policy before using the product. In order to present the privacy policy to secondary users, Mattel would need to direct every secondary user to a website, require that they read and consent to the privacy policy, and then provide a voice baseline with which to later authenticate the secondary user when using the product. This notice-and-choice scheme creates an absurd requirement in the fast-paced environs in which these products will be used.

Instead, producers of communications-capturing technologies should be permitted to freely collect secondary user communications. However, if producers of communications-capturing

16 18 U.S.C. § 2702(b)(3) (2012).

17 *See, e.g.*, *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *9 n.6 (N.D. Cal. Mar. 26, 2013) (explaining that the plaintiff may have pleaded himself out of a Stored Communications Act claim by alleging that Pandora was the intended recipient of plaintiff's personally identifiable information, since intended recipients can consent to third party disclosure under the Stored Communications Act without originator consent).

18 18 U.S.C. § 2702(b)(5).

19 *See also* Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, WASH. POST (Mar. 11, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves ("Hello Barbie works by recording a child's voice with an embedded microphone that is triggered by pressing a button on the doll. As the doll 'listens,' audio recordings travel over the Web to a server . . . . That information is used to help form Hello Barbie's responses.").

technologies decide to collect secondary user communications, they must distinguish between primary and secondary user communications on the back end. Companies that successfully distinguish between primary and secondary user communications can treat primary user communications in accordance with their privacy policies, but should be required to adhere to strict use and disclosure restrictions with respect to secondary user communications. Companies that fail to distinguish between primary and secondary user communications should be required to treat all of their recorded communications as belonging to secondary users. This framework encourages the adoption of innovative communications-capturing technologies while protecting secondary users, who do not consent to the back-end use and disclosure of their communications as described in privacy policies.

IV. Conclusion

We should be troubled by the rise of communications-capturing technologies and their effect on secondary users. Surreptitiously recording communications without consent has long been viewed as a privacy violation. Additionally, there may be many secondary users for every device purchased by a primary user, suggesting that secondary users comprise a much larger constituency to consider when developing privacy standards for these devices. While there may be debate over the significance and extent of the privacy protections secondary users should be afforded, protections should be fully considered before the ubiquity of communications-capturing technologies outpaces the law's ability to respond. As the use of communications-capturing technologies grows, so too will the importance of designing privacy protections with secondary users in mind.

You're Invited! ABA Programming

Recent Developments in Consumer Protection Networking Event

August 3, 2016, 8:30 – 10:30 am EST

The panel will be composed of enforcers from the FTC, State Attorney General's office, an U.S. Attorney's office, as well as a private practitioner. The panelists from the state and federal government agencies will discuss recent developments and notable cases and trends in government enforcement. The private practitioner will discuss cyber security/privacy issues and offer insight as to how best to avoid scrutiny and respond to a government investigation

Moderator:
- Lori Perrin Lustrin

Speakers:
- Cindy Liebes
- Adrienne Rabinowitz
- Sarah L. Shullman
- James Ward

In-Person Location:
Bilzin Sumberg Baena Price & Axelrod LLP
1450 Brickell Avenue, Suite 2300, Miami, FL 33131

Click here for more information and to register.

Member Benefit: Access Past Committee Program Audio Recordings

The Section of Antitrust Law's Committee Programs are informal educational events on timely topics that typically last 60-90 minutes. As a benefit to Section members, these Committee Programs are available in an MP3 format at no charge. Section members can download the MP3 file to their computers and transfer the content to a portable MP3 player (such as an iPod or other digital audio player) or burn it to a DS.

To listen to or save a Committee Program, click here.

Who Watches the Watchmen? The Rise of Data Brokers and the Need for Transparency

By Andrew Stanley, University of Iowa College of Law

I. Introduction

Today is an age of "Big Data." The last 20 years have seen significant rise in the controversial industry of data collection. "Data Brokers" track and sell personal information such as a consumer's previous online purchases and social media activity. This information is packaged and sold to advertisers, corporations, and other parties who then resell the data. This growth has created some difficult questions. What are the legal ramifications of a data breach that results in the exposure of data? What happens if data brokers sell data, and the sale results in identity theft? What options should consumers have to protect their data? While the industry has grown exponentially, the legal framework has not followed pace.

Over the last few years, some states have begun amending their consumer protection laws.[1] The federal government has not taken any major steps forward in passing legislation to ensure proper safeguards for consumers' private information.[2] As data collection grows, so too has its infringement on privacy rights. The current response has been far too muted, and direct oversight is needed to better guide the ever-increasing scope and influence of Big Data.

II. The Rise of the Data Broker

A. Who are the data brokers?

The FTC has defined three types of data brokers:

> (1) entities subject to the Fair Credit Reporting Act (FCRA)[3]; (2) entities that maintain data for marketing purposes; and (3) non-FCRA covered entities that maintain data for non-marketing purposes that fall outside of the FCRA, such as to detect fraud or locate people.[4]

Although the first type of data broker is subject to FCRA, the other two categories of data broker are not subject to the same degree of regulatory oversight.

Regardless of the category, all data brokers are intermediaries between a consumer and a corporation, collecting and selling personal information.[5]

A majority of the time, personal information is collected without the consumer's knowledge because the data is obtained through a variety of sources, sometimes unwittingly communicated by

---

1 *Infra* Part II.A.3

2 *Infra* Part II.A.1

3 This statute governs how credit reporting agencies handle credit information. Entities subject to these requirements include Transunion, Equifax, and Experian, but can also include individuals who collect and sell credit information (such as background check organizations). *See* Fed. Trade Comm'n, *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations*, at 1-5, REPORT (July 2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

4 Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and Accountability*, at i, REPORT (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

5 Fed. Trade Comm'n, *FTC to Study Data Broker Industry's Collection and Use of Consumer Data*, NEWS RELEASE, (Dec. 18, 2012), http://www.ftc.gov/opa/2012/12/databrokers.shtm.

the consumer.[6] Collections of data, what I will term a "portfolio", are made of "propensities," with each propensity relating to an isolated fragment of consumer personal data.[7] Data brokers collect propensities from a remarkable array of sources, including social network activity, public surveys, online shopping, and data purchased from other data brokers.[8] Information has become big business, with leading data brokers amassing propensities from nearly a billion consumers around the world, and offering portfolios to over 7,000 clients.[9] Buyers of this information include retailers, insurance agencies, credit card issuers, government agencies, trade groups, and politicians. The true extent is unknown, as data brokers refuse to divulge specific clients.[10]

Perhaps the most well-known anecdote used to describe the scale of modern data tracking comes from a New York Times article, focusing on retail giant Target's use of advertising algorithms to determine that a woman was pregnant, thereby "appropriately tailoring" the marketing materials she was sent. However, the woman lived with her parents, and her father was unaware of his daughter's pregnancy.[11] The advertisements ultimately led to an embarrassing confrontation between Target, the father, and the daughter. Another widely known example of data monitoring includes seemingly omniscient online advertisements that update to reflect recent searches and browsing history.[12]

Big Data and the data brokers that make up the industry are on the rise, and anyone who can use such data will support the continued tracking of personal information. Regardless of how one feels about the process on an ethical or moral level, there is a clear lack of transparency, oversight, and legal guidelines necessary to protect consumers who are unequipped and uniformed of how their data is collected and sold.

III. What Legal Structures Are Currently in Place?

The current legal framework around data brokers is a mixture of common law tort, federal financial and healthcare disclosure policies, and state data use limitations.[13] However, laws on combatting Big

---

6 Much of the information is tracked by websites for these data brokers, which can give an extensive look into a consumer's behavior patterns. *See* Michal Kosinski et al., *Private traits and attributes are predictable from digital records of human behavior*, PNAS (2012), http://www.pnas.org/content/110/15/5802.full (demonstrating that "likes" on Facebook can give insight into "sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender.").

7 Acxiom 2014 Annual Report, ACXIOM (2014), http://files.shareholder.com/downloads/ACXM/0x0x763250/A1DBFBD8-E136-4701-B0F2-3DC695E5ED08/acxiom2014_Annual_Report_FINAL_RRD_PDF_.pdf (stating that their capabilities include sourcing "over 3,000 propensities for nearly every U.S. consumer).

8 Acxiom alone reported collecting information from public sources such as "property and assessor records, motor vehicle records, driver's license records . . . and court records. . ." as well purchasing data from other data brokers who that directly monitor consumer behaviors. *Id.*

9 *Id.*

10 Letter from Acxiom, Data Broker, to Representative Edward J. Markey, U.S. Representative (Aug. 15, 2012), https://web.archive.org/web/20130302024214/http:/markey.house.gov/sites/markey.house.gov/files/documents/Acxiom.pdf

11 Charles Duhigg, How Companies Learn Your Secrets, NY TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1.

12 About Google Ads, GOOGLE, https://support.google.com/ads/answer/1634057?hl=en, ("¶T]he ads you see may be based on what you searched for, your location, and the time of day.").

13 Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 16, FTC REPORT (Mar. 2012),

Data were not drafted or intended to cope with the current state of the industry.

A. A Tangled Web Woven

1. Federal Apathy

Federal laws surrounding the transfer and disclosure laws apply to banking and financial institutions, and the healthcare industry.[14] These statutes were not intended to regulate the collection data, or any part of the Big Data industry; they instead deal only with certain information security and breach notification policies. Therefore, they address only a narrow subset of the information collected by the Big Data machine, chiefly financial and health records. However, data collection reaches information far beyond these records. These statutes do not affect propensities and portfolios not directly related to healthcare or credit; it is up to self-regulation to tackle these propensities and portfolios, with almost no federal oversight.[15] While bills have been proposed to address a growing data industry, none have gained any serious traction.[16] Currently the only real federal enforcement of Big Data comes from the myriad statutes enforced by the Federal Trade Commission.[17]

2. The FTC's Stance

In 2014, the FTC released a report fully analyzing the issue of data brokers. While it acknowledged some benefits to the industry, such as more closely tailored advertising and reduced risk of fraud, it identified several issues that the Commission felt need addressing at the federal level.[18] One such issue was transparency.[19] Consumers have their personal information collected and stored without any knowledge of what their portfolio looks like, or what propensities are inside it. At the federal level, data brokers are not required to put any transparency measure in place for consumers, and there is no "opt-out" mechanism. The FTC used the example of a consumer whose portfolio suggests they are a motorcycle enthusiast.[20] On the one hand, this would allow local motorcycle dealerships to send coupons and targeted advertisements. On the other hand, this information could be used by an insurance agency to quote higher rates because the consumer's portfolio gives an impression of liking to engage in risky behavior.[21] The consumer would have no say in the insurance company's conclusion; the consumer may not even know that he is receiving different treatment from the insurance company based on his purchasing and search history.

---

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

14 This includes Fair Credit Reporting Act (FCRA), the Gramm Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH).

15 *Congress Considers Regulating Data Brokers*, SKIPEASE (April 20, 2015), http://www.skipease.com/blog/data-brokers/congress-regulate-data-brokers.

16 FTC, *supra* note 4, at 7. Some more cynical commenters have surmised that this is due to the cozy relationship those with political power have with some data brokers, i.e. Big Data helps re-election campaigns. *See generally* Nathan Abse, Innovations in Web Marketing and Advertising: Big Data and Microtargeted Political Advertising in Election 2012: The Challenge Ahead, IAB PRESENTS, http://www.iab.net/media/file/IAB-Big-Data-and-Microtargeted-Political-Ads-in-Election-2012.pdf.

17 *See, e.g.*, the list of consumer protection statutes providing enforcement power to the FTC. https://www.ftc.gov/enforcement/statutes. This too is an odd fit, however, as the authority requires the enforcement to stem directly from a three-part test, and by the time the practices of data brokers are self-evident enough to uniformly fit the test, the harm to consumers will likely already have taken its toll.

18 FTC, *supra* note 4, at 47–48.

19 *Id.*

20 *Id.*

21 *Id.*

A second (and more pressing) issue is data security. Data brokers rarely delete the consumer data that they maintain, even as it becomes obsolete.[22] The risk of less-than-honest parties obtaining personal information from portfolios, either through hacking or through legal means is high, potentially leading to an increased rate of consumer identity theft.[23] The FTC felt that these issues presented significant harm to consumers, and that the best course of action was to increase transparency and create oversight that provides consumers with more control over their data.[24]

3. State Consumer Protection Laws

The state response to Big Data is growing, but still does not directly address the key issues, including transparency. What many of the laws *do* address, however, is safeguards and liability regarding potential breach or illicit use of consumer data. California in particular has taken aggressive steps towards combatting such issues.[25] The general approach of these safety measures is best represented by three California state privacy laws: the so-called "Shine the Light Law,"[26] the data security obligation law,[27] and the breach notification law.[28]

California's "Shine the Light Law" imposes a disclosure requirement for data brokers with regard to any third party who buys or shares portfolios.[29] This at least allows consumers to learn how their data is used by submitting a request for the information.[30] The data security obligation law requires data brokers to take reasonable steps to destroy records no longer in their position, addressing the identity theft concerns.[31] Finally, the breach notification law requires data brokers to inform any consumer whose data they have collected of any security breach or unauthorized use of their data.[32] Taken together, these three laws provide a valuable foundation of consumer protection, but there are still potent flaws in each, as well as in the system on the whole.

One limitation is that not every state regulates Big Data in the same manner, meaning some citizens receive less protection over their data then others. Furthermore, the internet makes it increasingly simple for a business in one state to collect data from a consumer in another, and the choice of law and forum issues that arise out of such a situation is bound to complicate potential civil litigation and any related remedies available to consumers.[33]

---

22 The rationale behind this permanent storage is ease of identity authentication.

23 Dr. Trevor W. Nagel, *FTC Settles with Data Brokers in Sale of Consumer Data Used for Illicit Purposes*, WHITE & CASE (Mar. 15, 2016), http://www.whitecase.com/publications/article/ftc-settles-data-brokers-sale-consumer-data-used-illicit-purposes; Gregory Maus, *How Corporate Data Brokers Sell Your Life, and why You Should be Concerned*, THE STACK (Aug. 24, 2015 at 2:27 pm), https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned.

24 FTC, *supra* note 4, at 50.

25 In addition to laws, California also setup the "Office of Privacy Protection" (now a division of the California Attorney General). *See* www.privacy.ca.gov.

26 Cal. Civil Code §§ 1798.83–1798.84.

27 Cal. Civil Code § 1798.81.5.

28 Cal. Civil Code § 1798.82.

29 Cal. Civil Code §§ 1798.83–1798.84. These requirements include providing the information provided to third parties, as well as the identity of those third-party buyers.

30 Cal. Civil Code §§ 1798.83(a)

31 Cal. Civil Code §1798.81.

32 Cal. Civil Code §1798.82.

33 Currently, issues are often settled with the FTC, but as the industry grows in complexity that may not also be an easy fix.

Additionally, consumers still have little choice in the collection of their data. There are few options for a consumer to "opt-out" of data collection, or to know the breakdown, content, or implications of the data collected. While transparency is of some use, this value is stunted by consumers' inability to know what inferences that third parties may draw from these propensities.

In addition, the procedure to determine who is using data can be clunky. A consumer may not know at the outset which company is collecting data, and would have to obtain the information through a retailer or simply send multiple requests.[34] A better solution would be to create a central access point where a consumer could see a pseudo-profile, or score, with information (such as who is buying data) readily available. Another solution would allow consumers the ability to access their data portfolio directly, verify such data or request the removal of certain data.

Despite some shortcomings, state laws are at least slowly addressing the more pressing issues and loopholes involved in Big Data. However, a federal policy would not only provide a more robust umbrella of protection for consumers, but also provide a guideline for increased uniformity in state laws.

IV. The Need for National Transparency

Despite the risks associated with large-scale collection of data, and the adoption of privacy requirements in state consumer protection laws, there has yet to be any concentrated federal legislative efforts directed at regulating this increasingly large business. With the current system evoking images of a patchwork fix, direct federal regulation would promote increased transparency, as well as more uniform security protocols. As with credit scores and do-not-call lists, this reform should provide consumers with information about their portfolios and third party buyers, and options to determine how their personal information is used.[35] This could be accomplished either through an independent agency to which data brokers are required to report, or by establishing private data "agencies" similar to those consumer reporting agencies ("CRAs") who manage and collect information for determining an individual's FICO score.[36] A centralized system would allow consumers to easily and fluidly monitor their data and ensure its accuracy. This would also facilitate control over the dissemination of private information such as health issues, familial status, religious affiliation, and sexual orientation.[37] This type of system is necessary, as there are currently serious holes in data verification. If a data broker

---

34 *See, e.g.*, Bloomingdales reporting system, *Bloomingdale's and bloomingdales.com Notice of Privacy Practices*, BLOOMINGDALES (Apr. 26, 2016), https://www.customerservice-bloomingdales.com/app/answers/detail/a_id/357/~/bloomingdales-and-bloomingdales.com-notice-of-privacy-practices. A consumer would potentially need to undergo this process with every retailer they frequent.

35 Privacy Rights Clearinghouse, *Credit Reporting Basics: How Private Is My Credit Report?*, PRIVACY RIGHTS CLEARINGHOUSE (Rev. April 2016), https://www.privacyrights.org/how-private-my-credit-report; Fed. Trade Comm'n., *Information for Consumers: The National Do Not Call Registry*, FTC.GOV, https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry.

36 These include Experian (who coincidentally is also a large data broker), TransUnion, and Equifax. CRAs are in turn subject to regulations through the Fair Credit Reporting Act. Indeed, the FCRA provides a great mirror for how such an act to regulate data brokers could look. The parallel is helpfully served by the fact that data portfolios are becoming more and more like a supplement to a consumer's credit score.

37 Such control over private information draws parallels to the national no-call list, or HIPPA. The individual consumer gets a say over how their privacy is interrupted or how their information is stored, except when it is information that is cumulatively drawn from patterns of behavior.

buys information collected from retailers, it could reflect a purchase made not by the consumer, but someone who borrowed or stole this or her credit card, creating an inaccurate perception of the consumer. There is also the issue of increased data collection centered on children and teens, who may grow up with an entire portfolio reflecting behavior made not as adults, but as teenagers, forgivable indiscretions included.[38]

The law should also put forward increased oversight over the methods and length of data storage. It is unclear what legal liability may arise from a breach of privacy from a portfolio held by data brokers.[39] While some states are tackling this issue by updating their own consumer protections laws, such changes are not widespread or uniform enough to stem the risks.[40] A federal consumer protection law aimed at the business practices of data brokers would protect consumers from having their data used for illicit purposes, and create the proper legal remedies necessary to ensure adequate security.[41]

V. Conclusion

Big Data does not seem to show any signs of slowing. There are potential benefits from the collection and transmission of data, but that does not mean consumers should have no say in how their information is used. Therefore, a real addition to the national consumer protection laws can prevent the risk of consumer harm posed by the collection of their data.

Like what you see in this edition?

Want to get more involved?

Please contact Ashley Rogers at arogers@gibsondunn.com

---

38 The habits and purchases made as a teenager should not serve to set the foundation for how I am perceived in my late 20s to data brokers.

39 *See* Maus, supra note 25 ("The current lack of oversight not only allows criminals and arguably private companies to abuse personal data, but it may pose a national security threat. . . . The current opaque data broker market could allow China and other governments to simply buy the information they want without having to steal it, particularly as the models for extrapolating data become ever more accurate.").

40 Mathew Ingram, *FTC: Privacy Self-Regulation Not Enough, "Do Not Track" Needed*, GIGAOM (Dec. 1, 2010, 12:15pm), https://gigaom.com/2010/12/01/ftc-privacy-do-not-track; *Data Brokers in Regulatory Crosshairs*, FENWICK & WEST (Feb. 28, 2014), https://www.fenwick.com/publications/pages/data-brokers-in-regulatory-crosshairs.aspx; Angelique Carson, *Data Brokers Demystified: A Call for Ethics*, IAPP (Sept. 18, 2014), https://iapp.org/news/a/data-brokers-demystified-a-call-for-ethics.

41 These are not unfounded concerns. *See* Nagel, *supra* note 25.

Data Leaks and Privacies Breached: Security and Privacy Concerns Posed by the Internet of Things

By JD Moore, Pennsylvania State University—Dickinson Law

Much like the introduction of the smart phone, the proliferation of the "Internet of Things" likely represents the next evolution of internet-connected technology.[1] The term Internet of Things ("IoT") is a catch-all phrase referring to everyday objects that are connected to the Internet and interact with the environment or other objects.[2] Unlike previous internet-connected devices, IoT devices transmit data without human intervention.[3] While the IoT industry is still in its infancy, IoT technologies have demonstrated the potential to embed objects with sensors and internet connectivity: for example, vehicle-to-vehicle communication is being researched and developed with the goal of reducing traffic accidents attributable to human error;[4] Amazon's Dash button lets users order household products simply by pressing a Wi-Fi connected device; and wearables, such as FitBit, allow for the collection of extensive data about the user's physical activity.

The IoT will provide convenience and safety to many consumers as more devices become interconnected. However, this new era of Internet-based technology presents a host of potential privacy concerns, as there is currently no federal regulation concerning the collection of data by IoT devices.[5] In 2015, the Senate Committee on Commerce, Science and Transportation showed bi-partisan support for allowing IoT to remain unrestricted, citing the success of the 1990s dot-com era.[6] Yet the current legal framework for consumer privacy is inadequate to cope with the problems presented by the IoT.[7] Two notable issues arising from the IoT are the risk of consumers being specifically identified through data collection[8] and the security of consumers' devices.[9]

I. Identity through Data Collection

Given the enormous amounts of data collected by IoT devices, many consumers wish to keep their data private from device manufacturers or third parties. However, manufacturers wish to monetize the data by selling data to data brokers who, in turn, sell data to companies for various purposes.[10] To balance these competing desires, companies have begun "de-identifying" data.[11] De-identification is a

---

1 Jayavardhana Gubbi et al., *Internet of Things (Iot): A Vision, Architectural elements, and Future Directions*, 29 FUTURE GENERATION COMPUTER SYS. 1645, 1646-47 (2013); Liz Coll & Robin Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection*, Consumers International, Apr. 2016, at 4.

2 Coll & Simpson, *supra* note 1, at 6-7.

3 *Id.* at 8; Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS. 14, 14 (2016).

4 *See* https://www.technologyreview.com/s/534981/car-to-car-communication/.

5 Melissa W. Bailey, Note, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, 94 TEX. L. REV. 1023, 1032-33 (2016); https://iapp.org/news/a/senate-committee-explores-internet-of-things-regulation/.

6 *Id.*

7 Williams, *supra* note 3, at 15; Christin S. McMeley, *Protecting Consumer Privacy and Information in the Age of the Internet of Things*, 29-FALL ANTITRUST 71, 71 (2014).

8 *Id.* at 1029-32; Williams, *supra* note 3, at 14-15.

9 Coll & Simpson, *supra* note 1, at 31-32; Williams, *supra* note 3, at 15.

10 *See* http://www.cnbc.com/2015/12/12/price-of-wearable-craze-your-health-data-hacked.html; Bailey, *supra* note 5, at 1025-26.

11 Yianni Lagos, *Taking the Personal Out of Data: Making Sense of De-Identification*, 48 IND. L. REV. 187, 187 (2014).

process that allows manufacturers to collect data without any specific references to a single individual (e.g. removing a name, address, or phone number).[12] While de-identification seems to be a workable compromise, data may be "re-identified".[13] Re-identification occurs when nonspecific data (e.g. gender or location) indirectly identifies a specific individual.[14] For example, if John is the only male with a January 1st birthday within a general location, then a person or company could reasonably infer that this data belongs to John, even though none of this data by itself specifically identifies John. Re-identification may also be easy to achieve, especially where a dataset is small.[15] To use the previous example, re-identifying John within a dataset containing 100 other males will likely be easier than re-identifying John within a dataset containing 10,000 other males, as the odds of John sharing a birthday and general location with another individual are greatly diminished.

The possibility of re-identification seriously undermines consumers' privacy interest in the IoT. For example, consumers expect the most amount of privacy within their homes. Yet, Samsung's SmartTV warned users that spoken words could be recorded and transmitted to a third-party through the television's regular data capturing methods.[16] Even more concerning, Siemens, a company that manufactures smart meters for electricity use within homes, stated:

> We, Siemens, have the technology to record [electricity use] every minute, second, microsecond, more or less live [. . .] From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data.[17]

Even outside of the home, consumers' specific locations can be identified through vehicle-to-vehicle communications.[18]

Aside from merely being identified, there is also concern for how this identification will be used. The ubiquity of sensors may facilitate increased government surveillance within otherwise protected areas.[19] Even if the government does not use the technology to examine individual homes, the government could use data collected from the IoT to establish a constitutional search of the home.[20] Moreover, re-identification could lead to types of discrimination.[21] Fitbit, for example, has sold de-identified employee data to employers.[22] Although Fitbit provides de-identified data, re-identification may reveal unhealthy habits or disabilities that could lead to adverse treatment in the workplace.[23] CVS has already required employees to provide "personal health metrics" such as weight and body fat composition, and an employer demanding Fitbit data would receive similar personal health information.[24]

---

12 *Id*. at 188.

13 *Id*. at 191-92.

14 *Id*. at 188, 192.

15 Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 132-33 (2014).

16 Williams, *supra* note 3, at 14-15.

17 *See* https://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things.

18 *See* https://iapp.org/news/a/senate-committee-explores-internet-of-things-regulation/.

19 Williams, *supra* note 3, at 21-22.

20 *Id*.

21 Peppet, *supra* note 16, at 117-18. *See* Bailey, *supra* note 5, at 1030-31.

22 *Id*. at 1025-26.

23 *Id*. at 1030-31; Peppet, *supra* note 16, at 118-19.

24 *Id*. at 119.

Compounding IoT's privacy problem is the current legal framework's inability to address the privacy implications arising from the enormous collection of data.[25] Current privacy laws generally rely on anonymization through the elimination of "personally identifiable information"[26]; however, this data also runs the risk of re-identification.[27] Fortunately, the Federal Trade Commission ("FTC") has recognized the privacy problems inherent in the IoT, and, in 2012, published a report aimed to guide companies in collecting data without compromising consumer privacy.[28]

Shortly after releasing the report, the FTC used its "broad enforcement authority under Section 5 of the FTC Act"[29] to file a complaint against HTC America, a company specializing in smartphone and tablets.[30] The complaint alleged that HTC America failed to implement the security necessary to protect consumers using the company's mobile phones.[31] Under the settlement, HTC America is required to develop and release software patches to fix vulnerabilities in the company's phones and establish a comprehensive security program to minimize the risk of further invasions of consumer privacy.[32]

II. Security of Consumers' Devices

Alongside consumer identification, the security of IoT devices is another major privacy concern.[33] Data breaches are an unfortunate side effect of Internet-connected technology from which even large corporations have not been spared.[34] Having personal information disseminated as a result of a data breach is troubling, but hackers attacking the IoT have the potential to achieve even more unsettling, or fatal, results. In November 2015, HP found that 60 percent of the most commonly used IoT devices have serious security vulnerabilities.[35] Hackers have already been able to access and publicize webcam footage and baby monitors,[36] and medical devices such as insulin pumps and pacemakers may be hacked.[37] As a result, these security risks undermine consumers' expectation of privacy.

Despite these risks, our current legal framework is unprepared for the security problems presented by the IoT.[38] Nothing requires manufacturers to adopt adequate security practices,[39] even though "experts have known for years" about the vulnerability of IoT devices.[40] Further complicating the issue is that most security research has been conducted at the

---

25 *See id.* at 132; Williams, *supra* note 3, at 15.

26 Peppet, *supra* note 16, at 132 (quoting Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1740-41 (2010)).

27 *Id.*

28 McMeley, *supra* note 7, at 72.

29 *Id.* at 71.

30 *See* https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile; *Id.* at 72.

31 *Id.* at 72.

32 *See* https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile.

33 Coll & Simpson, *supra* note 1, at 31-32; Williams, *supra* note 3, at 15.

34 *See* http://www.bloomberg.com/news/articles/2015-10-20/sony-to-pay-as-much-as-8-million-to-settle-data-breach-claims; http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

35 Williams, *supra* note 3, at 15.

36 Bailey, *supra* note 5, at 1025.

37 Williams, *supra* note 3, at 15; Peppet, *supra* note 16, at 134.

38 *See id.* at 15; McMeley, *supra* note 7, at 71.

39 *Id.* at 15.

40 Peppet, *supra* note 16, at 134.

back-end by researchers and hackers, instead of at the front-end by manufacturers.[41]

Specifically, laws governing security issues have been narrowly drafted and exclude some new technologies.[42] However, the situation may not be as dire as it appears. The enforcement gaps in our current laws and regulations have been quickly filled by the FTC.[43] When security lapses occur,[44] the FTC has used its broad authority under Section 5 of the FTC Act to penalize companies.[45] For example, in 2013, the FTC filed a complaint against TRENDnet,[46] a company specializing in networking hardware,[47] alleging that hackers were allowed to "tap into [TRENDnet's] Internet-connected cameras" as a result of "the company's lax security measures[.]"[48] The settlement requires TRENDnet to establish a comprehensive information security program that identifies security vulnerabilities and prevents future attacks.[49] Additionally, "TRENDnet is prohibited from misrepresenting the security of its cameras or the security . . . of the information that its cameras or other devices transmit."[50]

The FTC's enforcement authority should not be the sole protector of individual privacy and device security. More regulation is required to address privacy and security concerns in product design, rather than addressing consumer risks after a privacy invasion or security breach has already occurred. Fortunately, the government has recognized the substantial privacy and security risks posed by the IoT and appears ready to begin regulating it.[51] On March 15, 2016, the Senate unanimously adopted a resolution "which called for a 'national strategy' on development of the [Iot]."[52] Further, on April 27, 2016, the Developing Innovation and Growing the Internet of Things ("DIGIT") Act passed the Senate Commerce, Science and Transportation Committee.[53] The DIGIT Act represents a bi-partisan effort to "require [a] working group to report to Congress in one year on recommendations to 'appropriately plan for and encourage the proliferation of the Internet of Things in the United States.'"[54] The DIGIT Act's working group will study consumer protection issues posed by the IoT, as well as "the overall regulatory environment" of the IoT.[55]

While more regulation may be on the horizon, the process is just beginning. In the interim, consumers are left to rely on the will of the companies developing the IoT to ensure that their privacy interests are not ignored. However, while consumers may risk exposure on the front-end, the FTC's enforcement track record indicates that the Commission will not tolerate companies leaving consumers vulnerable. Thus, even though front-end regulation is possibly still years away, consumers may take some solace knowing that companies will not be permitted to recklessly disregard their privacy and security.

---

41 Williams, *supra* note 3, at 15.

42 McMeley, *supra* note 7, at 71. *See* Peppet, *supra* note 16, at 136.

43 *Id.* at 71. *See* Peppet, *supra* note 16, at 136

44 Peppet, *supra* note 16, at 136.

45 McMeley, *supra* note 7, at 71. *See id.*

46 Howard W. Waltzman & Lei Shen, *The Internet of Things*, 27 No. 7 INTELL. PROP. & TECH. L. J. 19, 19 (2015).

47 *See* http://www.trendnet.com/company/.

48 Waltzman & Shen, *supra* note 48, at 19.

49 *See* https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

50 *Id.*

51 Paul Merrion, *Senate Bill Lays Groundwork for Federal Oversight of Internet of Things*, CQ ROLL CALL, Apr. 28, 2016, at 1, 2016 WL 1694637.

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.*