Spring 2015

The Case for a Consumer Privacy Bill of Rights: A Study of Online Behavioral Advertising and Mobile Device Tracking

Andrew P. McChesney
Trinity College, andrew.mcchesney@trincoll.edu

THE CASE FOR A CONSUMER PRIVACY BILL OF RIGHTS: A STUDY OF ONLINE BEHAVIORAL ADVERTISING AND MOBILE DEVICE TRACKING

by

ANDREW PARKER McCHESNEY

A thesis submitted in partial fulfillment of the requirements for the Degree of Bachelor of Arts with Honors in Public Policy and Law

TRINITY COLLEGE

Hartford, Connecticut

Fall 2014-Spring 2015

Acknowledgements

First and foremost, this thesis would not have been at all possible without the guidance, support, and inspiration offered by Professor Adrienne Fulco. Never before have I come across a teacher who has challenged, encouraged, and brought out the best in me like Professor Fulco has. She instilled an intellectual curiosity that I will bring with me for the rest of my life. From the very beginning of this entire process, Professor Fulco has been by my side offering suggestions for further reading, helping me work through this complex argument, and supporting me in whatever I needed. I would never have started, nor come anywhere close to completing, this thesis without the constant guidance of Professor Fulco. I am, and always will be, profoundly grateful.

I also owe a great deal of gratitude to Professor Mark Silk, whose comments guided my final draft, and Professor Abigail Williamson, who worked with me from day one. Thank you to Erin Valentino who helped in my research and citations, and Rachael Barlow who was always an available resource. Thank you to Professor Ned Cabot, who helped convince me to come to Trinity in the first place, and has been a mentor ever since. Thank you to all of my Public Policy and Law colleagues who undertook this challenge with me, your excellent work drove me to do my very best.

Finally, and most importantly, thank you to my family. Without your guidance I truly would not be the person I am today. I lost two grandparents this semester, and without the support of my family I would not have been able to carry on and finish this task. I dedicate this thesis to my Grandmother, Grandma Mary, and my Grandfather, Nappo. While they are not here to see the final product, I know they are with me every day, proud of my accomplishments, and smiling down on me.

Table of Contents

Introduction

The Internet has revolutionized the world. Everyday life is vastly different now than it was just ten or fifteen years ago, due in large part to the technological advances that society has seen. Social interactions have gone online; social media and the rise of mobile computing has allowed an unprecedented level of connection to the world around us. Business has been transformed as well. While consumers used to browse products in the aisles of stores, this browsing now happens on the Internet. Consumers are increasingly relying on Internet connections to make purchases, browse competitors, and make decisions. There is no doubt that consumers have benefitted from the technological advances of the past fifteen years, but there is also no doubt these benefits have consequences. Smartphones and an Internet connection are now ubiquitous, and they are quickly becoming a necessity of everyday life.

With these changes come challenges. As consumers navigate the web on a desktop, smartphone, or other device, their movements are tracked. Whether it be a pair of shoes you searched for on Amazon.com, a health question you researched at WebMD.com, a political article you read on any number of websites, or even just a search engine query, at some point there is a company (or in most cases multiple companies) collecting this information. Data collection has become a ubiquitous tool for firms to create consumer profiles, and then monetize that information. The ubiquitous collection of personal data has, in many ways, funded the incredible explosion of innovation we have seen in the tech sector. Indeed, advertising and targeting models that use personal information to sell relevant ads pay for many of the 'free' services we use online.

At the same time, and in contrast to this ubiquitous data collection, Americans have always cherished some concept of "privacy." Although the Constitution does not specifically

articulate a right to privacy, themes of privacy can be seen throughout the Bill of Rights. The Fourth Amendment for example protects citizens' property or, "persons, houses, papers, and effects", from "unreasonable searches and seizures" by the federal government without a warrant.[1] While rights guaranteed in the Constitution have heavily influenced our notion of privacy, no general right to privacy exists against private actors. This is not to say that consumers have no interest in privacy. On the contrary, even without constitutional protection consumers have continually expressed interest in their privacy online. In essence a normative right has formed and defined by Deborah Stone in *Policy Paradox,* a normative right is not backed by the state, but rather by the normative values of society.[2] The Supreme Court has recognized certain areas of privacy, but has yet to address consumer privacy. Simply because a right to informational privacy, or consumer privacy, has never been clearly articulated, that does not mean we as a society do not value privacy.

This creates something of a paradox, however. While polls continue to show a consumer interest in privacy, we as a society have continued to engage in activity that puts our personal information at risk. Through social media, mobile connectivity, and other online avenues, consumers now offer up more and more of their information to be collected. We, as a society, need to find a way to balance these two competing values. On one hand we have the privacy interests of individuals, and on the other the interests of businesses around the globe who rely on our personal information to stay profitable. In this vein, I offer my thesis as an argument for Congress to pass a Consumer Privacy Bill of Rights, which could balance these competing interests and create an environment where both consumers and businesses benefit.

---

[1] U.S. Const. amend. IV.
[2] Stone, Deborah A., *Policy Paradox: The Art of Political Decision Making*. (New York: Norton, 2002) 350.

I am not the first, and most certainly will not be the last, to call for additional consumer protections online. In February 2012, the White House released *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Digital Economy*, a report that for the first time called for the creation of a Consumer Privacy Bill of Rights.[3] While I used this Consumer Privacy Bill of Rights as a framework, I will argue for a simplified version to be administered by the Federal Trade Commission (FTC). The Consumer Privacy Bill of Rights that I propose would recognize four rights of consumers: notice, choice, access, and security. These rights are taken from the Fair Information Practice Principles, which, as the next chapter will illustrate, have become the backbone of almost all data collection practices. As with any right, these are not and cannot be unlimited. Chapter One will make the case for the FTC to be given rule-making authority with respect to any privacy legislation. Different contexts bring about different privacy concerns, and the FTC should be the federal agency tasked with interpreting these rights and issuing context-specific regulations that not only protect consumers, but also promote innovation in industry.

Scholars around the globe have written about these issues and offered their own suggestions. There are those, such as Catherine Schmierer, who believe industry self-regulation and a continuation of the status quo is the best policy to protect consumers while still promoting innovation.[4] Others, however, like the authors of the White House report, have argued that industry self-regulation has failed to adequately protect consumers and baseline privacy protections are needed. I offer my thesis as a middle ground. I follow the work of Dennis D.

---

[3] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,* (Washington, D.C.: The White House, 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed October 1, 2014), 1.

[4] Catherine Schmierer, "Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation," *Richmond Journal of Law and Technology* 17, no. 4 (2011), http://jolt.richmond.edu/v17i4/article13.pdf (accessed October 1, 2014).

Hirsch, whose article, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation*, suggests co-regulation as a solution that both consumers and businesses can be happy with. As Hirsch writes, "Co-regulation encompasses initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards. It is neither pure government regulation, nor pure industry self-regulation, but rather a hybrid of the two."[5] While my thesis argues for the creation of a Consumer Privacy Bill of Rights, the implementation of these rights would need to be a process in which the concerns of both consumers and businesses are taken into account. Private industry has a huge role to play in consumer privacy and the best way to protect consumers is by engaging industry, and looking at some of best practices that already protect consumers.

One of the most interesting aspects of this topic is the speed at which things change. There are always new technologies that disrupt the status quo and have to be evaluated for their privacy implications. In the same vein, there are always new examples of both the benefits and harms to consumers that online activities pose. From a policy perspective, this means two things. First, as technology has thus far outpaced the law, it would make sense to have some baseline protections that can be adapted to new contexts and technologies. Second, it means there will always be room for new contributions to the policy debate. These issues are only going to evolve, and grow over time and an informed discussion will always be necessary.

I write this thesis, in part, as a consumer awareness tool. The vast majority of consumers are blissfully unaware of the huge industry that thrives on personal data, and if this paper can shed light on that it will be a success. I also, however, write this thesis to make the case for a

---

[5] Dennis D. Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle University Law Review* 34, no. 439 (2011): 440, http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr (accessed October 1, 2014).

Consumer Privacy Bill of Rights. To do so, I will examine two specific contexts to determine whether or not the existing regulatory framework adequately protected consumers, and therefore whether or not additional privacy protections are warranted. Chapter Two will scrutinize the online behavioral advertising industry, and the specific privacy concerns related to that context. I will then study the mobile context, and the unique benefits and challenges that come with it in Chapter Three, and again analyze whether or not additional privacy protections are warranted as a result. Finally, in the Conclusion I will discuss the future outlook of privacy protections; what emerging technologies are likely to contribute to privacy concerns in the future; and the likelihood that a Consumer Privacy Bill of Rights, or similar baseline privacy protection, will be passed by Congress in the near future.

Chapter One - FTC and Rulemaking Authority

As part of the case for Congress to pass baseline consumer privacy protections in the form of a Consumer Privacy Bill of Rights, this chapter will argue that the Federal Trade Commission should be given explicit rulemaking authority with respect to such legislation. Any form of legislation that attempts to regulate the Internet will need an agency to interpret the statute and issue regulations in line with the protections extended through legislation. Because privacy concerns vary with the context in which they are considered, the principles laid out in the Consumer Privacy Bill of Rights must be applied differently to different actors in different contexts. Mobile devices raise different privacy concerns than online behavioral advertising, and any agency that enforces the Consumer Privacy Bill of Rights must take this into account and enforce the principles accordingly. It is clear that not all data collection techniques are equal, and not all Internet firms pose the same threat to consumers as others. It should therefore also be clear that any legislation that attempts to regulate companies that do business on the Internet should be flexible enough to allow for the unfettered innovation that has thus far characterized the Internet age. It is with this understanding in mind that I write to argue that the FTC is the sole federal agency capable of balancing the competing interests of individuals and private corporations in the Internet space, and that they should be given rulemaking authority to enforce any proposed privacy legislation. This chapter will explain the history of how information collection practices have been regulated in this country, and show why the FTC is in the best position to issue context specific regulations in line with a Consumer Protection Bill of Rights. It will argue that while the FTC has attempted to protect the privacy of consumers under the authority of Section 5 of the FTC act, this authority is under attack, and the agency requires more rulemaking ability if it is to adequately protect consumers from the information collection

practices of commercial entities. The case studies that follow this chapter will not only demonstrate the need for consumer privacy legislation, but also illustrate the benefits of trusting the FTC with rulemaking authority with respect to such legislation.

History of Regulating Information Collection

Before explaining why the FTC is the ideal federal agency to promulgate regulations in response to the Consumer Privacy Bill of Rights, it is important to understand how, thus far, the commercial collection of user information has been regulated. Julia Lane, Victoria Stodden, Stefan Bender, and Helen Nissenbaum offer excellent background on the history of information privacy concerns in their book, *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Digital privacy concerns originated with the expanded "computer based record-keeping operations" in the 1970s, especially regarding large institutions such as banks and the federal government. In response, Fair Information Practice Principles (FIPP) were developed that have now become the cornerstone of privacy law.[6] Originally released in 1973 by the Department of Health, Education, and Welfare as a way to handle the data they administered, FIPP has been slightly modified since, and has become the backbone of information collection practices. The principles that are now followed by industry stakeholders are notice, choice, access, and security.[7] These have shaped how commercial entities treat user data, as well as FTC enforcement.

The nineteen seventies also saw the passage of the Fair Credit Reporting Act ("FCRA") and other sector-specific laws, as privacy concerns were mainly relevant to financial information

[6] Julia Lane et al., *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge, UK: Cambridge University Press, 2014), 5- 6.
[7] Lane, et al., 7.

and government record keeping.[8] A 2011 Congressional Research Service report on Personal Information stated, "There is no comprehensive federal privacy statute that protects personal information. Instead a patchwork of federal laws and regulations govern the collection and disclosure of personal information and has been addressed by Congress on a sector by sector basis."[9] These specific sectors include: consumer credit reports, electronic communication, federal agency records, education records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, children's online information, and customer financial information.[10] Jeffrey Rosen in *The Unwanted Gaze: The Destruction of Privacy in America*, articulates how this patchwork of regulations came to be:

> Although polls about privacy show that a majority of people claim to support it, many of the best interest groups strenuously oppose it. Corporations dislike privacy protections that would restrict their ability to use personal information in marketing schemes. Lobbyists for federal law enforcement are also powerful foes of privacy reform…As a result, the politics of privacy tends to be largely reactive, fired by heartstring-tugging anecdotes that capture the public imagination.[11]

Motor vehicle records, for example, were only regulated after the murder of actress Rebecca Schaeffer. She was murdered by an obsessive fan who found her address using state drivers license records. In response, Congress passed the Driver's Privacy Protection Act, which forbids states from releasing certain personal information such as, Social Security Number, photo, age, and addresses.[12]

---

[8] Lane, et al., 6.
[9] Gina Stevens, *Privacy Protections for Personal Information Online* (CRS Report No. R41756) (Washington, DC: Congressional Research Service, 2011), 2, http://www.fas.org/sgp/crs/misc/R41756.pdf.
[10] Stevens, 2.
[11] Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000), 170.
[12] Rosen, 170.

Role of FTC

Issues of consumer privacy are nothing new to the FTC, and the agency has a history of enforcing data collection practices under their limited authority from section 5 of the FTC act. While the agency has been at the forefront of promoting consumer privacy protections, it has lacked the relevant authority to enact rules and regulations that would allow consumers a baseline of privacy protections. After the proliferation of the Internet brought vast changes to consumer habits as well as societal norms, and without a guaranteed right to privacy, consumers were left exposed to the data collection practices of private companies. Regulation fell to the FTC, which was established in 1914 through the Federal Trade Commission Act and has a mission to, "protect consumers and promote competition."[13] As the main consumer protection agency in the United States, the

> FTC's efforts to protect consumer privacy date back to the 1970s, when it began enforcing one of the first federal privacy laws – the Fair Credit Reporting Act ("FCRA"). Since then, the Commission has sought to protect consumer privacy through law enforcement, policy initiatives, and consumer and business education. Using these tools, the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace.[14]

In this way, the FTC has become the de-facto government agency for commercial privacy regulation.

---

[13]"Our History," *FTC.gov*, Accessed October 17, 2014, http://www.ftc.gov/about-ftc/our-history.
[14]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf, ii-iii.

Section 5 Authority

Without explicit authority from Congress to regulate information collection, the FTC has relied on its authority under Section 5 of the FTC act to protect consumers from "unfair or deceptive acts" :

> The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that "**unfair or deceptive acts or practices** in or affecting commerce...are...declared unlawful." (15 U.S.C. Sec. 45(a)(1)). Safe Web amended Sec. 5(a) "unfair or deceptive acts or practices" to include such acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States. "Unfair" practices are defined as those that "cause[] or [are] likely to cause **substantial injury** to consumers which is **not reasonably avoidable** by consumers themselves and **not outweighed by countervailing benefits** to consumers or to competition" (15 U.S.C. Sec. 45(n)).[15]

The FTC can only bring about enforcement action when there is (a) substantial injury; it is (b) not reasonably avoidable; and (c) not outweighed by countervailing benefits. While the FTC was never specifically tasked with regulating consumer privacy or collecting personal information, the agency assumes this power under Section 5. When Congress passed the FTC Act in 1914, it left unfair practices broad for this very purpose:

> It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task.[16]

---

[15] "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," *FTC.gov*, July 1, 2008, http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[16] Gina Stevens, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority,* CRS Report No. R43723, (Washington, DC: Congressional Research Service, 2014), http://fas.org/sgp/crs/misc/R43723.pdf, 8.

In this way, without explicit authorization from Congress to regulate the information collection practices of commercial entities, the FTC has relied on the powers of Section 5 to become the de facto government agency tasked with protecting consumers online.

The FTC has been unable to enact meaningful consumer privacy protections because it lacks the explicit authority from Congress to do so. Although the agency has been a key player in the development of industry best practices and self-regulation, it has been limited in its ability to enforce any policy that falls outside unfair or deceptive practices. The agency has developed two models of enforcement that it has used thus far to promote consumer privacy to the best of its ability using Section 5 authority. Without a congressional mandate to regulate the information collection practices of private firms, the FTC has done the best they can under Section 5.

These two models of enforcement are the notice and consent model, and the harm-based model. Historically, the FTC has focused on consumer protection online in terms of two of the Fair Information Practice Principles mentioned earlier: notice and consent.[17] The FTC was largely concerned that firms were providing notice and consent to consumers about their information collection practices. The FTC would only step in and bring about enforcement action when companies failed to provide notice or consent. The FTC hoped "that notice and consent would provide a market mechanism for encouraging industry self-regulation of data privacy."[18] The notice and consent model allowed the FTC to bring about enforcement action when a company failed to provide notice about information collection practices, or when a company failed to obtain consent from a user to collect information. Crucial to this notice and consent model, however, is the assumption that "citizens are able to assess the potential benefits and

[17] Lane, et al., 8.
[18] Lane, et al., 8.

costs of data acquisition sufficiently accurately to make informed choices."[19] But can citizens actually make informed choices? According to the authors of *Privacy, Big Data, and the Public Good,* the answer is no. The assumption of informed choice, they write, "is most certainly a legal fantasy today, for a variety of reasons including the increasing use of complex and opaque predictive data-mining techniques, the interrelatedness of personal data, and the unpredictability of potential harms from its nearly ubiquitous collection."[20] The FTC has suffered from this notice and choice model, focusing on whether or not companies post a privacy policy or not, and whether or not that privacy policy is followed. The FTC has not taken the role of evaluating whether or not these privacy policies actually convey meaningful awareness or consent.[21] As Catherine Schmierer remarks in her article titled, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation,* "[I]t is...widely believed that consumers do not read these policies, because either they are uninterested or feel the documents are written in legalese and, thus, are incomprehensible...Nonetheless, even if consumers do not read online license agreements, privacy policies, or terms of use, they could be bound by their terms."[22] Under Section 5, the agency can only hold companies to the policies they promulgate; the agency cannot set its own standards for clear and meaningful privacy policies. The FTC lacks the authority under the FTC act to enforce rules that would require meaningful awareness or consent.

This shortfall has not been overlooked by the FTC itself. In the 2012 report "Protecting Consumer Privacy in an Era of Rapid Change," the FTC recognized the shortcomings of the notice and consent model: "Specifically, the notice-and-choice model, as implemented, has led to

[19] Lane, et al., 8.
[20] Lane, et al., 8.
[21] Lane, et al., 22.
[22] Schmierer, 13.

long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[23] The problem is that even with an understanding of the shortfalls of the notice and consent model, the FTC is powerless to enact meaningful change. Explicit authority from Congress to enforce the Consumer Privacy Bill of Rights, would allow the FTC to make rules and regulations that would allow consumers to receive meaningful notice of information collection practices, and therefore express meaningful consent.

In addition to the notice and consent model, the FTC has relied upon the harm-based model for enforcement action. The harm-based model protects consumers by focusing on protecting "consumers from specific harms – physical security, economic injury, and unwanted intrusions into their daily lives."[24] Essentially, in the harm-based model, the FTC would wait for specific harms to occur to consumers, and then retroactively bring enforcement action against negligent firms under Section 5 authority. Much like the notice and consent model, the harm-based model did not escape criticism. The harm-based model has been criticized "for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored."[25] The FTC has been forced to adopt this model, as they are unable to issue specific regulations that could address these criticisms without authority from Congress.

Using a notice and consent approach in conjunction with a harm-based model, the FTC has attempted to create an environment where the privacy interests of consumers are protected, while private companies can still have the flexibility to innovate and respond to the market. They

---

[23] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, 18.

[24] *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* (2012), 18.

[25] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* (2010), iii.

have done so solely under their authority to regulate unfair or deceptive practices under Section 5 of the FTC act. The FTC recognizes that neither model is perfect: "both models have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers."[26] Yet the agency has been unable to enact more meaningful change without expanded authority from Congress.

Challenge to FTC Authority, *FTC v. Wyndham Worldwide Corp.*

The FTC has relied on authority under Section 5 of the FTC act to bring enforcement actions against private firms and to regulate data collection practices as well as data security measures. This authority, however, has recently been challenged in court in a case that could undermine the agency's ability to regulate these practices. The FTC alleged that Wyndham Hotel and Resorts violated Section 5 by misrepresenting the security measures they provided for customer information. According to the agency:

> The case against Wyndham is part of the FTC's ongoing efforts to make sure that companies live up to the promises they make about privacy and data security. In its complaint, the FTC alleges that Wyndham's privacy policy misrepresented the security measures that the company and its subsidiaries took to protect consumers' personal information**,** and that its failure to safeguard personal information caused substantial consumer injury. The agency charged that the security practices were unfair and deceptive and violated the FTC Act.[27]

---

[26] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* (2010), iii.

[27] "FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information," *FTC.gov*, June 26, 2012, http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

While most companies when faced with an FTC enforcement action "settle by way of a consent order, or otherwise,"[28] Wyndham did not settle. Rather, it challenged the FTC's authority under Section 5 to regulate security practices absent specific legislation.[29] Wyndham feels that the FTC has significantly over-stepped their statutory authority under section 5 of the FTC Act. The case was first heard by U.S. district court in New Jersey that rejected Wyndam's claims and found that the FTC did in fact have ample authority under Section 5 to bring data security enforcement actions against private firms.[30] Wyndham immediately appealed and the case is currently before the United States Court of Appeals for the Third Circuit.[31] This case will have far-reaching implications, implications that could potentially reach the Supreme Court. It is too early to tell where this case is going but it is fair to say that a decision against the FTC would significantly undermine or possibly eliminate the agency's ability to enforce not only data security measures,but also data collection practices under Section 5. If the FTC were to lose authority to regulate data security and data collection measures consumers would be left in an even more perilous position than they are in now. The FTC has thus far relied almost exclusively on their authority under section 5 of the FTC Act to protect consumers online, and this case further shows that the agency needs increased authority explicitly from Congress so there will be no doubt as to the agency's authority to regulate data collection, and security.

---

[28] Robert V. Hale II, "Recent Developments in Mobile Privacy Law and Regulation," *Business Lawyer* 69, no. 1 (2013): 293.
[29]"Third Circuit Hears Oral Arguments in FTC v. Wyndham," *Hunton & Williams*, March 5, 2015, https://www.huntonprivacyblog.com/2015/03/05/third-circuit-hears-oral-arguments-ftc-v-wyndham.
[30] *FTC v. Wyndham Worldwide Corp.,* 2:13-cv-01887-ES-JAD (D.C. NJ 2014).
[31] *FTC v. Wyndham Worldwide Copr.,* no. 14-3514 (3rd. Cir. 2014).

Conclusion

Any proposed privacy legislation, including the Consumer Privacy Bill of Rights, requires a federal agency not only to promulgate context-specific rules and regulations that protect the rights of consumers laid out in such legislation while not unduly burdening businesses, but also to enforce compliance with such legislation. The FTC is that federal agency. In the absence of comprehensive consumer privacy protection, the FTC has relied upon their limited Section 5 authority to become the de facto government agency responsible for protecting consumers in the digital marketplace. This authority must be expanded. The FTC should be tasked with developing and enforcing rules and regulations that respect the rights of individuals laid out in the Consumer Privacy Bill of Rights. It has the ability to issue context-specific regulations that protect the rights of individuals while allowing businesses to innovate and compete in the digital marketplace. Through its history in regulating the information collection practices of commercial entities, the FTC became educated about the industry, understands the different positions of stakeholders, and has become the federal agency best suited to enforce the Consumer Privacy Bill of Rights. It is time to recognize the role of the FTC in shaping consumer privacy policy thus far, understand their limitations under Section 5, and entrust them with the appropriate authority to enact meaningful change. The current authority of the FTC to regulate in these important fields is under attack, as evidenced by *FTC v. Wyndham Worldwide Corp.* This case illustrates the fact that the agency requires expanded authority from Congress. If courts were to decide against the FTC on appeal, consumers would be left in an even worse position than now. The FTC is the proper agency to enforce regulations surrounding data collection and security, and it is time for Congress to ensure the agency has the ability to do this. The case studies that follow will not only provide ample evidence that baseline privacy legislation is

needed, they will also illustrate the need for, and the benefits of, trusting the FTC with rulemaking authority under any consumer privacy legislation.

Chapter Two - Case Study on Online Behavioral Advertising

This chapter will examine the Online Behavioral Advertising (or OBA) industry and, using specific examples, demonstrate how thus far industry self-regulation has inadequately protected consumers. I will use this case study to illustrate that without formal consumer privacy protections, such as the Consumer Privacy Bill of Rights, consumers have been left to the mercy of every Internet company they come in contact with. As the Internet economy grows, and more and more purchases are made online, firms are increasingly looking for ways to capture this information and use it to their advantage. Whether by tracking browser history to suggest another purchase, using your likes and interests collected from unrelated websites across the Internet to produce an ad, or selling your information to interested third parties, companies are increasingly relying on Internet tracking technologies to increase their revenue. I will show that the basic principles laid out in the Fair Information Practice Principles that include notice, choice, access, and security, have been routinely overlooked or purposefully circumvented by private Internet firms in this process. Choice has become obsolete, notice inadequate, access non-existent, and security measures often inadequately protective of user data. Consumers need specific protections codified in law, and an examination of the OBA industry will make that case. I will scrutinize tracking technologies that rob consumers of notice and choice; self-regulating trade associations whose voluntary nature undermines their very goals; and the current state of do-not-track. This will make the case that self-regulation has not adequately protected consumers in the OBA context, and that the FTC should be given increased authority from Congress to regulate this industry more strictly.

Online Behavioral Advertising

Behavioral advertising can be defined as " the tracking of consumers' online activities in order to deliver tailored advertising."[32] This definition actually combines two distinct and important aspects of the OBA industry: tracking and targeting. Tracking can be defined as the processes through which companies actually collect user information across the web. Targeting, on the other hand, is the process in which this user information is actually analyzed, aggregated, and used to serve a particularly relevant advertisement to a particular user. For example, with ad-blocking software you can prevent the targeting aspect of OBA, i.e. you will not see an ad, but that does not actually address the underlying issue of tracking. It is important to keep in mind the distinction between tracking and targeting as each presents a different set of issues, yet they are often combined and misunderstood in the public discourse.

When tracking and targeting are used together, the result is an online behavioral advertisement. I am sure everyone reading this is familiar with these ads whether you realize it or not. If I were to search for a new set of headphones, for example, on Amazon.com, I would then be "followed" by advertisements for headphones related to that search across the Internet. It allows companies to tailor ads directly to the personal interests of specific consumers. These advertisements pay for much of the "free" online services we use:

> Behavioral advertising, for instance, allows content providers to fund the delivery of web-based content and services to consumers on the Internet. One way of providing web-based content is to require consumers to pay directly for the service (a 'subscription-based' approach). Another is to follow the broadcast television model of allowing advertising to pay content providers for providing a service to consumers (an 'advertising-based' model). The advertising-based approach is advantageous for both advertisers and consumers. Behavioral advertising, as compared to other forms of advertising, offers advertisers an efficient method of precisely targeting a valuable demographic…Indeed, behavioral advertising is already being used to aggregate a

[32] Federal Trade Commission*, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf, 7.

> commodity - consumer information - that, to the individual consumer, has little exchange value into a valuable product that allows the consumer to access relevant and free Internet content.[33]

Thus far, for the majority of commonly used sites the advertising-model has been used. Checking the weather at weather.com, or looking at yahoo.com does not require a subscription because they rely on the sale of relevant ads to pay for the content they provide.

This collection and aggregation of personal information has many privacy advocates up in arms, groups such as the Electronic Frontier Foundation, as well as individual scholars such as Dustin D. Berger (author of the article *Balancing Consumer Privacy with Behavioral Targeting*) have written about the potential dangers of OBA and offered solutions. The concern is not so much related to the targeting aspect of OBA, but to the tracking and the detailed profiles that result. For example, the Electronic Frontier Foundation writes:

> [O]ur concern here is not advertising but privacy against online tracking: protecting consumers against the largely invisible, poorly understood, and continually escalating surveillance of their online activities...[O]nline surveillance raises significant civil liberties concerns given the potential for government access to information about consumers held by businesses....[T]his information can be used to identify online users and discover their reading, viewing, associational and consumption choices.[34]

Privacy advocates, for lack of a better term, argue that the Fair Information Practice Principles, which, as stated in the previous chapter, became the backbone of almost any privacy protection of notice, choice, access, and security are not respected by companies that participate in OBA. Dustin D. Berger summarizes the position of privacy advocates nicely in his article, "Balancing Consumer Privacy with Behavioral Targeting," stating:

---

[33] Dustin D. Berger, "Balancing Consumer Privacy with Behavioral Targeting," *Santa Clara High Technology Law Journal* 27, no. 1 (2010): 31.

[34]"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Preliminary FTC Staff Report) Response of the Electronic Frontier Foundation," Electronic Frontier Foundation, https://www.eff.org/files/ftccommentseff.pdf.

> First, consumer and privacy advocates criticize behavioral targeting because it results in the compilation of a sizable array of potentially sensitive data about the consumer that exists outside her ability to protect, control, or monitor... In creating this picture, the profiler learns and potentially communicates something private about the consumer he has not authorized the profiler to know… Secondly, sometimes this unauthorized picture can be embarrassing, regardless of whether it is disclosed inadvertently or intentionally… Even worse, in the wrong hands, a consumer's profile could facilitate financial fraud or identity theft… Finally, consumer and privacy advocates also fear that the use of behavioral profiles to make decisions that may be inappropriate (or at least surprising) uses of consumer data. For instance, insurers or potential creditors might wish to use a consumer's profile in an attempt to establish pricing for their products.[35]

The principal concerns of privacy advocates surround the creation of detailed consumer profiles. Profiles that have been created without the full understanding of the consumer, are much more personal than consumers would assume, and that are outside of user control. These detailed profiles could potentially contain false information that the user cannot correct, and could then be used in employment decisions or insurance pricing. They also contain what many consumers would view as deeply personal or intimate information; for example, they could contain browser searches related to medical conditions, political affiliation, or sexual orientation – information that can be collected through an individual's browser history.

In contrast, industry representatives argue that self-regulation and the implementation of industry best practices will more effectively balance the competing interests of consumers who are looking for privacy and the interests of Internet firms. They are likely to argue that user information is not used in a manner inconsistent with consumer expectations, that consumers benefit from this tracking, and that absent specific instances of harm, increased regulation is unwarranted. They are likely to see any legislation or increased FTC authority as unnecessary and harmful to innovation. Catherine Schmierer summarizes these arguments in the conclusion

[35]Berger, 20.

of her article, "Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation":

> The existing system of self-regulation allows the FTC to utilize a flexible approach to enforcement as new technologies and methods of behavioral advertising increase in popularity and create privacy concerns...even though privacy advocates argue that it took the industry too long to take online consumer privacy seriously, regulators should wait and see if the industry's efforts are successful in creating widespread transparency regarding online advertisers' data collection practices. The FTC should also give the industry time to educate consumers, by providing clear privacy notices and showing consumers how they can control how data about their online activities is collected and used… Based on recent industry efforts, the FTC can do all of these things now without the aid of additional rule-making authority or the assistance of new privacy legislation.[36]

In other words, any increased rule-making authority for the FTC or privacy legislation would be premature and unnecessary. Industry representatives are also likely to argue against increased regulation or the implementation of user rights on economic grounds. As Avi Goldfarb and Catherine E. Tucker found in their article "Privacy Regulation and Online Advertising," "[E]ven moderate privacy regulation does reduce the effectiveness of online advertising, that these costs are not borne equally by all websites, and that the costs should be weighed against the benefits to consumers."[37] Opponents of privacy regulation will point to the advertising-model and suggest that increased regulation could disrupt that model and force content providers to move towards a subscription-based model.

Tracking Technologies Deny Notice and Choice

In order to evaluate the validity of these concerns, we first must understand how companies are able to track users across multiple sites on the Internet. Enter the cookie. Originally developed in 1994 by Netscape as an e-commerce tool, cookies preserved user login

---

[36] Schmierer, 57.
[37] Avi Goldfard, and Catherine E. Tucker, "Privacy Regulation and Online Advertising," *Management Science* 57, no. 1 (2011):2.

data and shopping cart history, and the cookie has transformed into the default tracking mechanism of companies.[38] While just a small text file, cookies allow companies to collect and track a user's online path and therefore create a profile that reflects that path. Cookies are the most common tool used to accomplish the first half of OBA, the tracking. The information collected from cookies is then analyzed and used to deliver an ad that corresponds to some of that information collected. For the most part, cookies do not collect so-called personally identifiable information but rather tie a user to a unique identification number which is then tied to a specific device, such as a laptop, phone, or iPad.[39] Through this anonymization, "profilers have attempted to mitigate some of the harm to consumers… behavioral advertisers, during public hearings and proceedings before the FTC, expressed their belief that information that does not identify a consumer's identity poses no significant risk to the consumer's privacy"[40] In this way, behavioral advertisers have argued against regulations because they claim data that is not linked to a specific person can cause no privacy harms. While true that an anonymized data set would not raise the same privacy concerns of one that contained social security numbers, for example, "even in datasets where this obviously identifying information has been removed, it is remarkably easy to identify users."[41] There is just so much data available that mitigation through anonymization is a myth at best, a flat-out lie at worst. The rich profiles compiled on consumers through tracking technologies clearly raise significant privacy concerns. The fact is, these profiles can be used to identify individuals, and therefore the information in the profiles will be tied to that individual.

---

[38]John Schwartz, "Giving the Web a Memory Cost Its Users Privacy," *The New York Times*, September 4, 2001, http://www.nytimes.com/2001/09/04/technology/04COOK.html.
[39]*FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 2.
[40]Berger, 28.
[41]Berger, 29.

Cookies offer the first piece of evidence that companies engaged in tracking do not respect user choice, and do not respect user consent. There are multiple types of cookies, and cookies are not the only piece of technology deployed by companies to track users. Putting it simply, there are traditional cookies which can easily be managed or deleted in a browser setting, and then there are more persistent cookies (flash cookies) which are not. As consumers started developing cookie blocking methods, advertisers developed new tracking technologies.[42] With flash cookies, "advertisers can continue to track individuals uniquely even if the user deliberately tries to avoid web tracking."[43] These flash cookies which re-spawn even when deleted, prove companies are more interested in collecting your information than respecting your choice when it comes to tracking:

> First, users cannot fairly be said to have notice of these activities. The entire point of new tracking methods seems to be to ensure that users are ignorant of them. The websites that used Flash respawning and cache ETag tracking did not disclose those practices in their privacy policies. Second, because these vectors are resistant to blocking, they rob consumers of choice. This undermines the advertising industry's representations about respecting individuals' choices and leaves consumers in a technical arms race with advertisers.[44]

Technology has been deployed that inherently robs users of notice and choice. A large part of the problem is the fact that, thus far, technology has greatly outpaced the law and regulators. Without backstop privacy protections, consumers have been left to deal with these invasive and manipulative tracking technologies on their own. A Consumer Privacy Bill of Rights would codify rights that have been the cornerstone of privacy protections since electronic privacy became a concern.

---

[42] Schmierer, 227.
[43] Chris Jay Hoofnagle et all, "Behavioral Advertising: The Offer You Cannot Refuse," *Harvard Law & Policy Review* 6, no. 273 (August 2012): 278.
[44] Hoofnagle et all, 291.

Cookies are not the only tracking technology deployed. There are also so-called "beacons" that "capture what people are typing on a website—their comments on movies, say, or their interest in parenting and pregnancy."[45] As Julia Angwin of the *Wall Street Journal* observed in 2010 as part of an investigative series into online tracking, "Tracking technology is getting smarter and more intrusive. Monitoring used to be limited mainly to 'cookie' files that record websites people visit. But the *Journal* found new tools that scan in real time what people are doing on a Web page, then instantly assess location, income, shopping interests and even medical conditions. Some tools surreptitiously re-spawn themselves even after users try to delete them."[46] The findings of the *Wall Street Journal* were echoed by the Electronic Frontier Foundation, whose webpage detailing the current state of do-not-track found, "[M]ore recent technologies have brought the advent of cookie-like tracking systems that are harder for a user to detect or delete, and may well provide marketers with a rich source of data about an individual. Today, online tracking companies use supercookies and fingerprints to follow people who try to delete their cookies, and the leakage of user IDs from social networks and similar sites has often given them an easy way to identify the people they were tracking."[47] The goal of these tracking technologies is simple: to collect user information no matter what. Even if a knowledgeable consumer is aware of tracking, and therefore regularly deletes cookies in order to avoid that tracking, that choice is ignored.

These technologies are deployed by almost all websites although network advertisers play a particularly important role. Network advertisers are "companies that select and deliver

---

[45] Julia, Angwin, "The Web's New Gold Mine: Your Secrets," The Wall Street Journal, July 30, 2010, http://www.wsj.com/articles/SB10001424052748703940904575395073512989404.
[46] Angwin.
[47] "Do Not Track," Electronic Frontier Foundation, https://www.eff.org/issues/do-not-track.

advertisements across the Internet at websites that participate in their networks."[48] Network advertisers illustrate how tracking is difficult for consumers to comprehend:

> This [cookies] allows the network advertiser to track the consumer's activities across multiple websites in the advertiser's member network and pay member websites when they supply consumers to the network advertiser. This behavior is hidden from the consumer; the consumer does not normally know anything about the cookies, which websites are members of which advertisers' networks, or what information a member website might share with the network advertiser."[49]

This problem is compounded by the fact that, "[a]n individual network may include hundreds or thousands of different, unrelated websites and an individual website may belong to multiple networks."[50] So while consumers are tracked across a variety of unrelated websites that belong to a network advertiser, they are virtually powerless to exercise any meaningful choice in regards to the tracking, and cannot be said to have significant notice of this tracking.

FTC and Industry Self-Regulating Trade Groups

As stated in the last chapter, without explicit authority from Congress to regulate the collection of personal information, the FTC has relied on Section 5 of the FTC act to protect consumers to the best of its ability. With authority to regulate only under Section 5, the FTC has been forced thus far to promote industry self-regulation as the best policy framework to protect consumers. Gina Stevens states in her 2014 CRS report:

> Initially, the FTC promoted industry self-regulation as the preferred approach to protecting consumer privacy. After assessing its effectiveness, however, the FTC reported to Congress that self-regulation was not working. Thereupon, the FTC began taking legal action against entities that violated their own privacy policies, asserting that

[48] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 3.
[49] Berger, 9.
[50] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 2.

> such actions constituted 'deceptive trade practices'... The FTC acknowledged that, although it had the power under section 5 of the FTC Act to pursue deceptive practices, such as a website's failure to abide by a stated privacy policy, the agency could not require companies to adopt privacy policies.[51]

The FTC lacks the authority to explicitly regulate the collection of user information online, rather they rely on the broad powers to regulate unfair or deceptive trade practices. Without this authority from Congress, the FTC has relied on self-regulation and holding companies to the privacy policies they post. The FTC is powerless, however, to stipulate what should be contained in a privacy policy, and in many cases this has resulted in very long privacy policies written in legalese that the public is unlikely to read, let alone understand. Herein lies one of the biggest problems for the FTC. Without explicit authority from Congress to regulate the collection of personal information, the FTC has been forced to use Section 5 authority that does not directly address this problem. Section 5 only allows the FTC to act after an unfair or deceptive trade practice has occurred, and it cannot enact rules that protect consumers from the beginning. The agency has been hampered by this lack of authority, and consumers have suffered as a result.

Without additional authority from Congress, the FTC was forced to promote industry self-regulation for online behavioral advertisers. In 2009, the FTC released the report, *Self-Regulatory Principles for Online Behavioral Advertising* ("FTC Guidelines"), as a way to promote and formalize industry best practices, even though the agency was unable to mandate the adoption of these principles.[52] The report recognizes both the benefits and threats to consumers that OBA presents:

> Participants at the Town Hall discussed the potential benefits of the practice [OBA] to consumers, including [a] the free online content that online advertising generally

---

[51] Stevens, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, 3.

[52] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), i.

> supports, [b] the personalized advertising that many consumers may value, [c] and a potential reduction in unwanted advertising. They also discussed the privacy concerns that the practice raises, including [a] the invisibility of the data collection to consumers; [b] the shortcomings of current disclosures about the practice; [c] the potential to develop and store detailed profiles about consumers; [d] and the risk that data collected for behavioral advertising – including sensitive data regarding health, finances, or children – could fall into the wrong hands or be used for unanticipated purposes.[53]

The FTC Guidelines attempt to address the concerns of privacy advocates while being flexible enough to allow for innovation in the industry. The FTC Guidelines laid out four main concepts for behavioral advertisers to address that largely reflect the four pillars of the Fair Information Practice Principles of notice, choice, access, and security. The first, control and transparency, calls for companies engaged in OBA to provide "meaningful disclosures to consumers about the practice and choice about whether to allow the practice."[54] This concept suggests that companies involved in OBA should still respect a user's right to notice and choice. Users should be notified of what information is collected and how that is used, and then be able to make a meaningful decision on whether or not to participate. The second concept advanced in the FTC Guidelines was for companies engaged in OBA to "provide reasonable data security measures"[55] to prevent breaches and to hold data only as long as the business interest requires. This concept reflects the security aspect of the Fair Information Practice Principles discussed earlier. The final two concepts also reflect the notice and choice aspects of the FIPP. The third concepts states: "[B]efore a company uses behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the consumer."[56] And the final concept presented in the FTC Guidelines requires companies to

---

[53] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), i.
[54] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 11.
[55] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 11.
[56] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 12.

"obtain affirmative express consent before they use sensitive data – for example, data about children, health, or finances – for behavioral advertising."[57]

These self-regulatory guidelines are a laudable first step, and if companies that use OBA were forced to comply, consumers would have a right to notice and choice. But without authority from Congress, these guidelines are just that, guidelines. Currently, the FTC is unable to mandate compliance, and it is up to individual companies to decide whether or not to abide.

This is not to say, however, that companies were not interested in following these self-regulatory guidelines. As Catherine Schmierer remarks in her article, "[T]he FTC hoped that the threat of regulation - should voluntary self-regulation not be successful in ensuring greater protection of online consumer privacy - would "scare" companies into taking self-regulation seriously."[58] With the threat of formal regulation over their head, the advertising industry quickly formed a trade association to self-regulate and impose the FTC guidelines upon itself, as a way to prove formal regulation is unwarranted.[59] The trade associations, however, actually highlight the need for increased FTC authority. Membership in a trade association is not necessary to conduct OBA, and therefore companies that decline to join a trade group that establishes best practices can continue to conduct OBA without any oversight. Trade associations may also find it difficult to enforce these standards, while the FTC could, if given the authority, mandate and enforce these standards.

One such trade association, The Digital Advertising Alliance (DAA), launched a website (www.aboutads.info) that, "most importantly, educates consumers about what online behavioral

---

[57] *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009), 12.
[58] Schmierer, 29.
[59] Reed D. Freeman Jr., Julie O'Neill, and Kimberly S. Robinson, "Industry Associations Launch Behavioral Advertising Self Regulatory Program Involving Icon," Morrison and Foerster, October 6, 2010, http://media.mofo.com/files/Uploads/Images/101006-Behavioral-Advertising.pdf.

advertising is and how they can control the collection of data regarding their online activity."[60] Consequently, the DAA introduced the "Power I" icon to address concerns regarding consumer notice and choice. The icon which is placed inside an advertisement allows consumers to know why they are seeing a particular advertisement and how to opt out of tracking (you can see an example above).[61] This opting out, however, would only be applicable to companies who are a member of the DAA. Before including the "Power I" icon on a webpage, a company must undergo an audit performed by a third party to ensure compliance with the self-regulatory guidelines outlined by the DAA. While joining the DAA is optional, "companies must also pay a registration fee and make a commitment, which may be enforceable by the FTC to comply with the industry guidelines."[62] In this way, companies that join the DAA must follow the self-regulatory guidelines or face FTC action under the deception principle in Section 5 of the FTC act. So companies that join a trade association can be held liable for not following the practices that membership requires; but again, membership is optional and companies that conduct OBA are not required to join.

DAA was not the only group to create an icon-based tool to help online advertisers comply with the self-regulatory guidelines. The case of TRUSTe, a for-profit company, illustrates the dangers of placing the burden of regulation on industry and not a Federal agency. TRUSTe, which originally monitored and certified privacy policies, created TRUSTed Ads – "a similar compliance program for the advertising industry" and, "like the DAA program, the

[60] Schmierer, 45.
[61] Schmierer, 45.
[62] Schmierer, 46.

TRUSTed Ads program utilizes an icon, which consumers can click on to access information regarding data collection for behavioral targeting purposes and 'an easy-to-use opt-out option.'"[63] In 2014, however, the FTC announced it had settled with TRUSTe over a complaint that the company did not in fact re-certify privacy policies and misrepresented itself as a non-profit company;

> The FTC's complaint alleges that from 2006 until January 2013, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals in over 1,000 incidences, despite providing information on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year.
>
> In addition, the FTC's complaint alleges that since TRUSTe became a for-profit corporation in 2008, the company has failed to require companies using TRUSTe seals to update references to the organization's non-profit status. Before converting from a non-profit to a for-profit, TRUSTe provided clients model language describing TRUSTe as a non-profit for use in their privacy policies.[64]

The very company that the public trusted to "self-regulate" in the OBA context has proven to be more concerned with profits than privacy. According to FTC Chairwoman Edith Ramirez, "TRUSTe promised to hold companies accountable for protecting consumer privacy, but it fell short of that pledge…Self-regulation plays an important role in helping to protect consumers. But when companies fail to live up to their promises to consumers, the FTC will not hesitate to take action."[65]

Trade associations that promote industry best practices do not adequately protect consumers from the harms that OBA poses. Membership in groups that promote and enforce self-regulatory standards are optional, and therefore there will always be companies outside of membership groups that are not required to follow any guidelines. The FTC can only take

---

[63] Schmierer, 46.
[64] "TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program," *FTC.gov*, November 17, 2014, https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.
[65] "TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program."

enforcement action against a company that is a member of a trade group and that does not follow that group's guidelines. They cannot, however, take enforcement action against a company that decides not to join a trade group. In this way, a perverse incentive has been created. To shield yourself from FTC enforcement action, it would make sense not to join a trade group and therefore be free to conduct OBA without any privacy protections in place, and without any oversight. In TRUSTe, we have seen a company that was supposed to protect consumers according to self-regulatory guidelines, but instead put profits over privacy. It is clear that in the OBA context, self-regulation is inadequate and the FTC needs additional authority and oversight to ensure consumers have the basic rights laid out in the FIPP: notice, choice, access, and security.

Do-Not-Track

Also included in the 2009 FTC guidelines for behavioral advertisers was an endorsement by the FTC for the creation of a so-called do-not-track mechanism. Do-not-track is a, "technology and policy proposal that enables users to opt out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. At present few of these third parties offer a reliable tracking opt-out, and tools for blocking them are neither user-friendly nor comprehensive. Much like the popular Do Not Call registry, Do-Not-Track provides users with a single, simple, persistent choice to opt out of third-party web tracking."[66] As the name implies, do-not-track is the idea that there should be a universal tool for consumers to be able to opt out of third party tracking if they so desire. Third party tracking is any tracking done

[66]"Do Not Track: Universal Web Tracking Opt Out," *Do Not Track*, http://donottrack.us/.

by a company outside of the domain which you visit. The Electronic Frontier Foundation explains:

> Many consumers understand that the websites they visit collect information about them, often for advertising purposes. But most consumers do not understand that when they visit those websites, other entities also collect information about them. The modern website typically brings together content from many different web servers and your browser assembles those pieces of content to display what looks like a single page from a particular branded entity. In this situation, however, your browser is actually requesting data from both that branded entity and many other "third party" servers—and all of those servers can get data from your browser at the same time.[67]

For example, if I were to visit yahoo.com, I would receive a cookie from Yahoo! for the purposes of remembering my login credentials, product fullfillent, or other "first-party" uses. Most likely, however, I would also receive cookies sent to me from companies other than yahoo. These "third-party" cookies are from firms that have a business relationship with yahoo, such as a network advertiser or analytic service, that are looking to collect my information. Do-not-track seeks to give users choice when it comes to third parties that collect your information, whether it be to use it for an ad or sell it to marketer.

Currently, do-not-track suffers from the same problem that characterizes the self-regulating trade associations. Without a mandate of compliance from the FTC or other regulatory agency, third parties are free to honor or ignore a do-not-track request as they see fit. Without universal acceptance of do-not-track, the idea fails. If all companies are not required to honor a do-not-track request, as is the case now, then the business incentive will actually be to ignore a do-not-track request, and consumer choice will again suffer. Do-not-track also suffers from the sudden explosion of so-called social plugins. These are the 'share' or 'like' buttons that you see on most web pages, but they also allow the parent companies (Facebook, Twitter, Google plus)

[67]"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Preliminary FTC Staff Report) Response of the Electronic Frontier Foundation."

to track you on unrelated websites; "Social media widgets (such as Facebook's Like button, Twitter's Tweet button, or Google +1's button) often track your reading habits. Even if you don't click them, the social media companies often see exactly which pages you're seeing the widget on."[68] Because you have a "first party" relationship with social media firms, they would claim to be exempt from do-not-track requests, which only block tracking from third parties. It is disingenuous to claim Facebook has a first party relationship with me when I visit a site unrelated to Facebook. This classification would only benefit the Internet giants such as Facebook, Google, and Twitter, that have both a first- and third-party relationship with consumers. Giving the FTC authority to mandate and regulate, the creation of a do-not-track would allow this loophole to be filled. If consumers want to opt out of third party tracking, the giant Internet firms should be forced to follow that choice as other third parties are.

It is also important to remember what a do-not-track policy would accomplish and what it would not. Although it would allow consumers to exercise choice as to the tracking done by third parties, it would not stop consumers from being served an ad. Without increased authority from Congress, it is hard to see how the FTC could mandate compliance with a do-not-track request. If we are serious about giving consumers meaningful choice about their online activity, we need a regulatory authority that is willing and able to mandate compliance with a do-not-track request.

[68]"Privacy Badger," *Electronic Frontier Foundation*, April 24, 2013, https://www.eff.org/privacybadger#social.

Conclusion

After analyzing the online behavioral advertising industry it is apparent that the current status quo of industry self-regulation has failed to adequately protect consumers. Through tracking technologies that rob consumers of notice and choice, self-regulating trade associations whose voluntary nature undermines their very goals, and the optional compliance of do-not-track requests, it is clear that consumers need their rights codified in law, and enforced through a Federal agency. The FTC is in the best position to understand the stakeholders and issue rules and regulations in line with legislation that allows for the continued growth of the Internet economy while at the same time respecting consumers and the choices they make. Regulation is not premature or unnecessary as industry representatives would have you believe. Rather, it is absolutely necessary in light of the fact that technology has thus far outpaced the law and regulators in ways that deny consumers meaningful notice and choice with respect to data collection practices. OBA, and tracking in general, create detailed profiles of consumers, profiles that can fall into the wrong hands, whether that be identity thieves or even the NSA. Consumers should have the right to make choices about those profiles, and companies should be required to respect these choices. While there are currently market solutions available for consumers, these solutions only work for the most technologically savvy and knowledgeable consumers. Ghostery, for example, is a browser extension that allows consumers the choice to "block all tracking easily, block tracking from particular companies, or choose to only allow tracking on the websites that they trust the most."[69] While Ghostery claims to have more that 20 million users,[70] the freedom that this extension offers consumers should be available to everyone, not just the consumers savvy enough to add the extension. Everyone uses the Internet, and everyone should

[69] "About Ghostery," *Ghostery.com*, https://www.ghostery.com/en/about.
[70] "About Ghostery."

have access to the choice that Ghostery, and other extensions like it, offer. Without a federal agency to mandate compliance, whether it be to the Fair Information Practice Principles or a do-not-track request, the incentives to businesses will continue to be to circumvent user choice and come up with ever-more imaginative ways to siphon user information no matter what choice the user has made.

Chapter Three - Case Study on Mobile Devices

Location, location, location. The phrase may come from real estate, but it proves just as true in the mobile device context. This chapter will examine the mobile device industry, and the privacy concerns that are related. In doing so, I will again show that consumers need baseline privacy legislation that codifies a user's right to notice, choice, access and security. Mobile computing is expanding rapidly, and to just give you an idea of how fast, look at these three statements.

1) "Last year's [2013] mobile data traffic was nearly 30 times the size of the entire global Internet in 2000."
2) "Average smartphone usage grew 45 percent in 2014."
3) "By the end of 2014, the number of mobile-connected devices will exceed the number of people on earth, and by 2019 there will be nearly 1.5 mobile devices per capita."[71]

All of these new devices, connected to the Internet, provide many of the same privacy challenges present in the OBA context (primarily the creation of detailed consumer profiles) but with one important extra piece of information: location. Smartphones and other mobile devices offer consumers tremendous benefits, many of which utilize locational information; but they also create privacy concerns that have yet to addressed. Technology has outpaced the law, and the mobile context might be the best example of this. This technology is so new and advancing so fast that consumers have been left unprotected, subject to the policies of whatever apps they have on their device, or of their service providers. Currently, there are no federal regulations that deal

[71] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019 White Paper," *Cisco.com*, February 3, 2015, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html.

specifically with information collected from mobile devices. I will argue in this chapter that in light of the privacy problems presented by mobile devices, a Consumer Privacy Bill of Rights, a bill that respects a user's right to notice, choice, access, and security, is necessary and proper to protect consumers not only in this context, but in all online activities.

Mobile Tracking Industry

Just as in the Online Behavioral Advertising (OBA) context, tracking of mobile devices offers consumers both benefits and potential dangers. The benefits of mobile tracking are largely summarized in a 2004 article, "Privacy Issues in Location-Aware Mobile Devices," by Robert P. Minch:

> There is little doubt that location-aware (sometimes also called location-enabled) mobile devices have enormous potential for enhancing safety, convenience, and utility in our lives. Already emergency services are being improved by the ability of responders to quickly locate persons making emergency calls on enhanced 911 cell phones or involved in accidents in location-aware vehicles. Parents can monitor the location of their children, who can summon assistance with a "panic button" on location-aware watches. Time and location-sensitive weather, traffic, and navigation information can be tailored to better meet the needs of users in specific locations. Even existing conveniences such as the ability to track package delivery from city to city may be enhanced to the extent that recipients are able to obtain precise estimates of delivery times and even track package locations as they are driven through the neighborhood to their house. Soon, consumers will benefit from many new offers of products and services that may be personalized and tailored based on their location and the locations of other entities that they deal with.[72]

When this article was written, mobile device technology and locational services technology were just getting started. The benefits mentioned have come to be, as marketers and advertisers have come to capitalize on these "new offers of products and services that may be personalized and

[72]Dr. Robert P. Minch, "Privacy Issues in Location-Aware Mobile Devices," *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 2004, http://www.computer.org/csdl/proceedings/hicss/2004/2056/05/205650127b.pdf, 1.

tailored based on their location…" As discussed earlier, mobile devices have increasing importance in the e-commerce economy because they are able to serve location-specific ads, which have increased rapidly recently. As Lauren Johnson of *AdWeek* put it, "The new hyper-targeted ad format is the latest move from the mobile advertising industry to capitalize on the growing interest in location-based marketing, which BIA/Kelsey estimates will bring in $4.5 billion this year. By 2018, per BIA/Kelsey, that number will grow to $15.7 billion."[73] The industry for location-based marketing services is expected to triple by 2018, and this industry is only likely to grow as more and more of our daily Internet activities take place on the go, which is exactly what is happening. A 2012 Pew Research Center poll found that 17% of cell phone owners "do most of their online browsing on their phone, rather than a computer or other device."[74] The 2013 FTC Staff Report on Mobile Privacy Disclosures makes three main points that summarize the privacy concerns that are presented from mobile device information collection:

> First, more than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user. This can facilitate unprecedented amounts of data collection. The data collected can reveal sensitive information, such as communications with contacts, search queries about health conditions, political interests, and other affiliations, as well as other highly personal information. This data also may be shared with third parties, for example, to send consumers behaviorally targeted advertisements.[75]

Mobile devices are inherently unique to an individual, and they differ from traditional Internet connections in that consumers bring mobile devices almost everywhere they go. This leads to an

---

[73] Lauren Johnson, "Does Mobile Marketing Actually Work in the Real World?" *AdWee,* November 4, 2014, http://www.adweek.com/news/technology/does-mobile-marketing-actually-work-real-world-161180.

[74] Aaron Smith, "Cell Internet Use 2012," *Pew Research Center,* June 25, 2012, http://www.pewInternet.org/2012/06/26/cell-Internet-use-2.

[75] Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf, 2-3.

unprecedented amount of user information that can be gathered from one device and tied specifically to a unique individual. Next the report finds the complexity of the mobile environment exceeds that of the desktop environment:

> Second, in the complicated mobile ecosystem, a single mobile device can facilitate data collection and sharing among many entities, including wireless providers, mobile operating system providers, handset manufacturers, application developers, analytics companies, and advertisers to a degree unprecedented in the desktop environment. This can leave consumers wondering where they should turn if they have questions about their privacy.[76]

Mobile devices and the explosion of 'apps' have created an ecosystem much more complicated than that found in the desktop environment. There are more entities that can access the vast information stored on a mobile device than are present in the traditional OBA atmosphere. Finally, the report details the location tracking concerns raised by mobile devices:

> Third, mobile devices can reveal precise information about a user's location that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers. Indeed, companies can use a mobile device to collect data over time and 'reveal the habits and patterns that mark the distinction between a day in the life and a way of life.' Even if a company does not intend to use data in this way, if the data falls in the wrong hands, the data can be misused and subject consumers to harms such as stalking or identity theft.[77]

Precise locational data is very sensitive and personal information, especially when collected over time. This information, a record of everywhere you have been with a mobile device, raises even more serious privacy concerns than data collected from desktop computers. Consumers could potentially be stalked or worse if this information is not properly secured.

These privacy concerns reflect many of the same concerns presented by OBA but in many ways they are more profound. Mobile devices can collect and store much more personal

---

[76] *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013), 2-3.
[77] *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013), 2-3.

information than a web browser, and they are always with us, sometimes collecting precise GPS location data. When profiles are created using locational data, they are significantly more invasive than those created by your browsing habits from a desktop. Mobile devices provide the opportunity for companies to follow you offline as well as online.

Consumers are aware of the increased privacy challenges that occur in the mobile context. This was confirmed by another 2012 Pew Research Center Poll that found that 54 perent of app users "have decided to not install a cell phone app when they discovered how much personal information they would need to share in order to use it."[78] It also found that 30 percent of app users

> have uninstalled an app that was already on their cell phone because they learned it was collecting personal information that they didn't wish to share…Taken together, 57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons… 19% of cell owners have turned off the location tracking feature on their cell phone because they were concerned that other individuals or companies could access that information.[79]

It is clear that even without any legislation to protect consumers in the mobile marketplace, interest in protecting user privacy in the mobile context is strong. While most consumers fail to understand the complex relationships and analytics that marketing and advertising firms use to serve ads on mobile devices, they still understand the vast and personal information that smartphones collect and have sought to exercise control over this information. One way firms enhance their own control is through the use of so-called "perma-cookies."

---

[78] Jan Lauren Boyles, Aaron Smith, and Mary Madden, "Privacy and Data Management on Mobile Devices" *Pew Research Center,* September 4, 2012, http://www.pewInternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

[79] Boyles, Smith, and Madden, "Privacy and Data Management on Mobile Devices."

Perma-Cookies

Traditional cookies and the tracking technologies discussed in the previous chapter often do not work as well on mobile devices. In part, this is because of the tremendous growth in apps. Cookies used on desktop computes look at an individual's Internet habits across multiple websites. However, on mobile devices a browser is often not used to access the Internet, and a specific app will communicate with the Internet. Because of this segmentation, firms were unable to track users across apps, and thus could only rely on cookies placed through browser apps. In response to this technical challenge, both AT&T and Verizon Wireless have recently come under scrutiny for adding so-called "perma-cookies" to user browser requests through a mobile device. AT&T has since stopped the practice because of public backlash,[80] or as Julia Angwin stated on ProPublica, "The move [AT&T stopping the use of 'perma-cookies'] comes after AT&T and Verizon received a slew of critical news coverage for inserting tracking numbers into their subscribers' Internet activity, even after users opted out."[81] Verizon Wireless continues to deploy these perma-cookies, however, as Jacob Hoffman-Andrews from the Electronic Frontier Foundation explains:

> Verizon Wireless has been silently modifying its users' web traffic on its network to inject a cookie-like tracker. This tracker, included in an HTTP header called X-UIDH, is sent to every unencrypted website a Verizon customer visits from a mobile device. It allows third-party advertisers and websites to assemble a deep, permanent profile of visitors' web browsing habits without their consent.[82]

---

[80] Juli Clover, "AT&T Stops Using 'Perma-Cookies' to Track Customer Web Activity," *Mac Rumors*, November 14, 2014, http://www.macrumors.com/2014/11/14/att-no-longer-using-perma-cookies/.
[81] Julia Angwin, "AT&T Stops Using Undeletable Phone Tracking IDs," *ProPublica*, November 14, 2014, http://www.propublica.org/article/att-stops-using-undeletable-phone-tracking-ids.
[82] Jacob Hoffman-Andrews, "Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls," *Electronic Frontier Foundation*, November 3, 2014, https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

Because traditional cookies do not work well on mobile devices, with all of the distinct apps, Verizon Wireless developed this technology to allow businesses to track consumers information across mobile devices and therefore serve better advertisments. “Like a cookie, this header uniquely identifies users to the websites they visit. Verizon adds the header at the network level, between the user's device and the servers with which the user interacts….unlike a cookie, Verizon's header is nearly invisible to the user and can't be seen or changed in the device's browser settings.”[83]

Similar to the choice denying flash-cookies mentioned in the previous chapter, these perma-cookies deny user choice by being inherently difficult to remove. They are potentially more hazardous because “the header ... affects more than just web browsers. Mobile apps that send HTTP requests will also have the header inserted. This means that users’ behavior in apps can be correlated with their behavior on the web, which would be difficult or impossible without the header.”[84] Verizon Wireless has developed technology to track consumers across different apps on the same mobile device, and to respond to the failure of traditional cookies on mobile devices. Many consumers may very well agree to this tracking in order to receive more personal ads, but the way in which Verizon Wireless has hidden it from consumers raises privacy concerns. In this example consumers were neither notified by Verizon Wireless of this practice, nor given meaningful choice as to whether or not to participate.

Verizon Wireless does allow consumers an opt-out mechanism but unfortunately “it appears that the opt-out does not actually disable the header. Instead, it merely tells Verizon not

---

[83] Jacob Hoffman-Andrews, "Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls."
[84] Jacob Hoffman-Andrews, "Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls."

to share detailed demographic information with advertisers who present a UIDH value. Meaningful protection from tracking by *third parties* would require Verizon to omit the header entirely."[85] Without a Consumer Privacy Bill of Rights, consumers have been subjected to the data collection practices of firms without any meaningful notice or consent.

Role of FTC in Mobile Context

The FTC suffers from the same problem the agency faced in the OBA context. Without any consumer protections codified in law, the FTC has been forced to rely on section 5 of the FTC Act to regulate data collection on mobile devices, and promote self-regulation as the best way to protect consumers. With that limitation, the FTC has nonetheless promoted consumer privacy through reports and guidelines that the agency releases. In February of 2013 the FTC released a staff report, *Mobile Privacy Disclosures; Building Trust Through Transparency*, which among other recommendations called for the creation of a mobile do-not-track mechanism.[86] The mechanism that the agency calls for in this report differs slightly from the do-not-track mechanism mentioned in the OBA context: "That ongoing effort [implementation of OBA do-not-track] would address both desktop and mobile web browsing, in contrast to the recommendation here, which would allow consumers to prevent tracking across apps."[87] A do-not-track mechanism that only requires browsers to comply would not work in the mobile context. Apps use the Internet all of the time in the mobile context, and it is vital that any do-not-track mechanism would apply to apps as well as browsers. Without increased authority from

[85] Jacob Hoffman-Andrews, "Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls."
[86] *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013), 21.
[87] *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013), 21.

Congress, however, the FTC will be forced to be a cheerleader on the sideline as the agency is now. The agency will have no power to enforce compliance with a do-not-track request and the entire of concept of do-not-track will fail.

Without legislation to enforce, the FTC has promoted self-regulation in the mobile context as well. In the 2013 staff report that focused on mobile privacy disclosures, the agency suggested mobile app developers follow the lead of self-regulation. The report recommends that "app developers should consider participating in self-regulatory programs, trade associations, and industry organizations, which can provide industry-wide guidance on how to make uniform, short-form privacy disclosures."[88] While these self-regulating groups offer consumers the best means of privacy control as this point in time, they are by no means adequate. As Kate Kaye from AdAge puts it:

> Ad industry self-regulators want mobile app developers to provide better notice of data collection and usage to consumers and...are unveiling guidelines for doing so. Both the Digital Advertising Alliance, which leads the industry's pervasive targeted ad privacy program, and the Network Advertising Initiative, which counts third party ad networks and exchanges as its members, are set to publish complementary new mobile data rules...Government is bearing down on mobile marketers and their data collection habits, and the ad industry aims to get out in front of the issue. However, despite the new guidelines, which will address how marketers notify users when data is collected via mobile apps, details for implementation and compliance monitoring remain undetermined...Enforcement is a ways off, too.[89]

Groups like the DAA and NAI, which were discussed in the previous chapter, will struggle to monitor all of their members and will be hesitant to employ meaningful enforcement actions.

---

[88] *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013), 24.
[89] Kaye, Kate. "Ad Industry Groups Intro New Rules for Mobile Data Collection." AdvertisingAge. July 24, 2013. http://adage.com/article/privacy-and-regulation/ad-industry-groups-intro-rules-mobile-data-collection/243261/.

The DAA and NAI will have slightly different roles in the mobile context, as Kate Kaye continues to explain:

> Digital Advertising Alliance members will be required to present users with a standard notice of mobile data collection for advertising purposes – most likely the DAA's AdChoices icon, a ubiquitous symbol in display advertising today. Clicking that icon will probably launch its own app which would let users choose whether to allow companies to collect cross-app data, location information and directory data.

Unfortunately without forced compliance through the FTC, initiatives such as the AdChoices icon will not adequately protect consumers. Consumers will only have the option to exercise meaningful choices if all of the stakeholders in the mobile ecosystem are treated in the same manner. The DAA and NAI guidelines will apply to different aspects of the mobile ecosystem:

> The NAI is unveiling a similar program today. While the DAA code applies to first-party data collection, the NAI's requirements are for its third-party ad network and exchange members which gather information across websites and mobile applications for ad targeting….It is unclear when either organization will actually enforce their new guidelines.

Critically, an enforcement mechanism was not specified in the guidelines nor was a timeline for implementation. Without these two crucial aspects, how can consumers expect to be protected by industry self-regulation? Industry representatives nonetheless see self-regulation as the ideal regulatory scheme:

> "I think that it's really incumbent on industry to get this right," said Mr. Groman [executive director and general counsel at the NAI]. "Policy makers on both sides of the aisle are particularly focused on mobile privacy and location privacy…. As we get more innovative I think it's really incumbent on us to bake privacy by design in from the start."[90]

[90]Kate Kaye, "Ad Industry Groups Intro New Rules for Mobile Data Collection".

There is no doubt that industry is vital in securing standardized privacy practices from the mobile context. The DAA and NAI have important roles to play, but enforcement is not one of them. Industry stakeholders need to be part of the policy making process, and they need to help develop the extent that consumers rights need to be respected in each context. However, we need an independent agency that has consumer interests in mind to enforce these standards.

In the mobile context, thus far the FTC has focused enforcement action on data security practices.[91] In part, this is due to the speed at which the mobile context has evolved. In a very short period of time smartphones have become ubiquitous, and regulation has struggled greatly to keep up. In addition to the 2013 staff report released by the FTC, the agency released "a new business guide that encourages mobile app developers to aim for reasonable data security."[92] This guide followed the announcement that the FTC had settled major charges with HTC America over their data security practices on mobile devices:

> ... [HTC America] failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk. The settlement with HTC America, announced by the FTC in February 2013, requires the company to develop and release software patches to fix vulnerabilities in millions of the company's devices. The company is also required to establish a comprehensive security program designed to address security risks during the development of HTC devices and to undergo independent security assessments every other year for the next 20 years.[93]

The FTC brought suit under its authority from Section 5, alleging that these practices of HTC represented an unfair or deceptive act because reasonable and necessary data security measures

---

[91] Hale II, 2.
[92] Hale II, 2.
[93] "FTC Approves Final Order Settling Charges Against HTC America Inc," *FTC.gov*, July 2, 2013, https://www.ftc.gov/news-events/press-releases/2013/07/ftc-approves-final-order-settling-charges-against-htc-america-inc.

were not followed. In this way, the FTC can retroactively enforce data security measures but only after the damage has been done. The FTC has struggled to bring enforcement action against the data collection practices of firms, in part because the technology is advancing so fast; and the agency wants to see how industry groups respond and self-regulate.

Conclusion

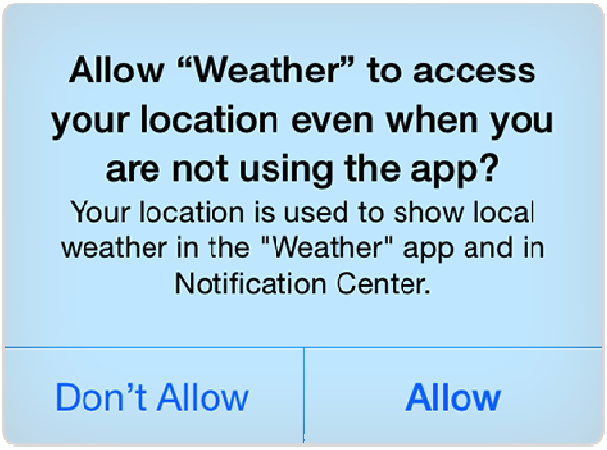
The mobile context is unique, and it is advancing everyday. The privacy challenges are complex and evolving with the technology, as is evidenced by a recent *New York Times* article by Stephanie Clifford and Quentin Hardy titled "Attention, Shoppers: Store Is Tracking Your Cell." The authors explain how retail chains have started to deploy technologies that actually track consumers as they move within the retail store:

> So last fall the company [Nordstroms] started testing new technology that allowed it to track customers' movements by following the Wi-Fi signals from their smartphones...Nordstrom's experiment is part of a movement by retailers to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn information as varied as their sex, how many minutes they spend in the candy aisle and how long they look at merchandise before buying it.[94]

In other words, the potential of mobile device tracking is just beginning to be realized. These issues are not going away. They will only get more pertinent as more and more firms look for business advantages resulting from mobile device tracking and the technology of mobile devices improves. Mobile device technology offers marketers, advertisers, and now even retail stores

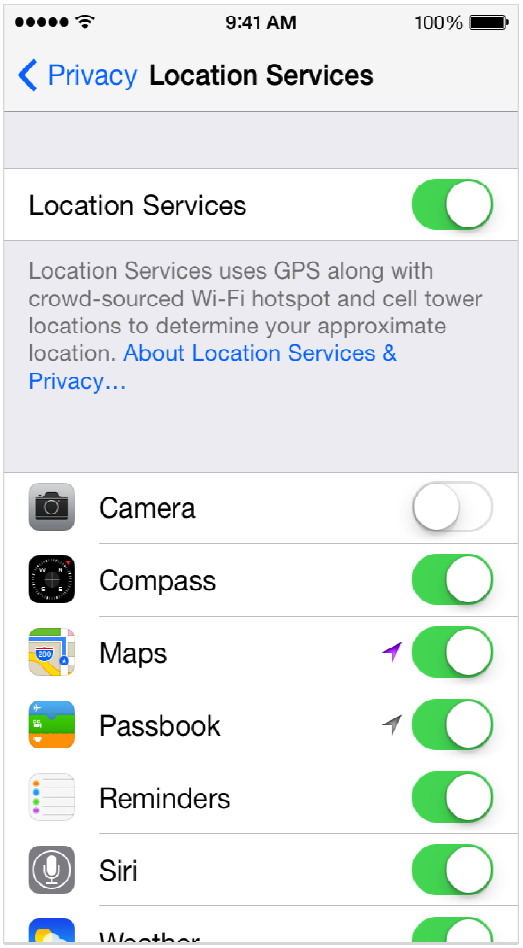
[94] Stephanie Clifford, and Quentin Hardy, "Attention, Shoppers: Store Is Tracking Your Cell," *New York Times*, July 14, 2013, http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0.

unprecedented new business opportunities, but at what cost? Consumers need baseline privacy legislation that would respect a user right to notice, choice, access, and security. As apps like Uber and Facebook use our personal data in more and more imaginative ways, we need oversight, and assurances that data will be collected and stored properly and in ways consistent with consumer choices.



There are market forces that have helped push the industry in ways that protect mobile privacy. iOS, the software that all Apple devices run on, has several features that help consumers manage privacy on their mobile device. Users can select exactly which apps can have access to locational data, iOS also allows users include a do-not-track request with Internet requests and notifies users (through an icon) when an application has recently used your location. On the right you can see two screenshots from iOS 8. The first shows how the software notifies and then asks for affirmative consent before an app begins collecting locational information. It then notifies and again asks for affirmative consent for the app to collect locational data when the app is running in the back ground. The second screenshot shows how iOS 8 allows users to decide exactly which applications have access to location services.

While these market solutions show that industry does have an interest in consumer privacy, they are not enough. As the Nordstrom example shows, companies are only going to increasingly rely on information that they can collect from consumer devices. These problems are not going away; rather, they are only likely to grow more acute as technology continues to advance in the mobile field. A Consumer Privacy Bill of Rights would ensure consumer trust in the industry and pave the way for the next wave of innovation in this exciting field. Obviously this technology has brought with it tremendous benefits, and as with most smartphone users, I would never want innovation in this field to be hampered by regulation. Having said that, users should have some baseline rights about their data – rights that can be defined within contexts by the FTC.



Conclusion

The Internet has changed the fabric of society. Never before have consumers had more information at their fingertips. At the same time, never before have private companies had more information on American consumers. The volume and intimacy of the information that private companies hold on consumers is only going to increase in the future as technology becomes more integrated into our daily lives. It is clear that the issues discussed in this thesis are not going away. They will only get more complicated as companies find more inventive ways to utilize the information they collect.

This examination of both the Online Behavioral Advertising context and tracking in the mobile context makes it clear that consumers have not been adequately protected by the current regulatory framework. Notice has become obsolete, as privacy policies and terms of use statements have become increasingly long and incomprehensible, often filled with legalese. This particular problem is only exacerbated in the mobile context as smaller screens means more and more pages of reading for the consumer. Consumer choice is often restricted or flat-out ignored, as flash cookies and perma-cookies specifically ignore user requests to block tracking. Self-regulating trade groups fail to offer consumers the privacy protections that they seek. In this light, I argue that a Consumer Privacy Bill of Rights with rule-making authority and enforcement by the Federal Trade Commission is the best way forward not only to protect the privacy choices of individuals, but also to promote trust in the online eco-system and spur both growth and innovation in the industry. I would create a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles of notice, choice, access and security. With these four basic rights, consumers could then look to the FTC to promulgate rules and regulations in line with the rights granted in a Consumer Privacy Bill of Rights. These rights would not and cannot be

absolute. Privacy concerns vary by context and consumer rights need to vary by context as well. The FTC is the federal agency capable of determining the extent and scope of each right within contexts. The fluid nature of technology lends itself to baseline protections that can be modified and adapted depending on the privacy challenges presented by new technologies.

Like any consumer protection regulation, a balance must be struck between two competing interests; the privacy interests of individuals and the legitimate interests of business. Thus far, this country has attempted to rely on self-regulation to achieve this balance. Supporters of industry self-regulation such as Catherine Schmierer would have you believe that industry has thus far adequately protected consumers and that any form of increased regulation would bring havoc and uncertainty to a booming data ecosystem. A look at our friends in Europe, however, proves otherwise. In contrast to the United States, the European Union has a comprehensive privacy law. As Laura Ybarra remarks in her article comparing our privacy laws with the E.U., "Currently, U.S. data collection laws are regulated by a patchwork system of state and federal laws and agencies. The E.U.'s 1995 Directive on Data Protection, on the other hand, mandated that each E.U. nation pass national privacy laws and called for the creation of a Data Protection Authority to protect citizens' privacy."[95] It is understood that the European Union has stronger privacy protections than we do in the United States. It is possible to move in the other direction, away from a patchwork of regulation that fails to protect consumers. It is possible to have comprehensive legislation that protects consumer rights, gives the FTC latitude in rule-making and enforcement, and continues to allow businesses to innovate.

The economic impact of any regulation would need to be studied. As Thomas Lenard and Paul Rubin make clear in an article that criticizes the FTC for failing to study the economic

[95] Laura Ybarra, "The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States," *Loyola of Los Angeles International and Comparative Law Review* 34, no. 267 (2011): 270.

impact of increased regulation, "The Privacy debate is taking place in an empirical vacuum. The FTC has developed policy recommendations without the benefit of systematic data on current privacy practices of firms or consumers, or systematic analysis of the benefits or costs of alternative privacy regimes."[96] If Congress were to pass a Consumer Privacy Bill of Rights, the FTC would need time to study the impact of the rules and regulations they would impose. It would be necessary to have industry stakeholders as part of the process to ensure that legitimate business concerns are accounted for. Before implementing any rules or regulations the FTC would need to understand the economic impact of the rules for specific contexts. A consumer's right to notice of data collection practices could impact the mobile context differently than the online behavioral advertising context, and the FTC would need to take this into account before issuing regulations. Thus far, the FTC has worked quite well with industry leaders and self-regulatory groups, aiding in the creation of self-regulatory guidelines. This relationship can and must continue into the future, especially in the agency is given rule-making authority with respect to privacy legislation.

While a Consumer Privacy Bill of Rights might well be an ideal solution to the United States data regulation problems, it is hard to see Congress enacting such legislation anytime soon. In February of 2015, the White House released a discussion draft of their proposal for a Consumer Privacy Bill of Rights, yet the bill has not been introduced in the 144th Congress, nor has the White House announced a congressional sponsor for the bill.[97] As Tony Romm from Politico puts it, "Lawmakers for years have failed to overcome disagreements to pass a

---

[96] Thomas M. Lenard, and Paul H. Rubin, "The FTC and Privacy: We Don't Need No Stinking Data," *The AntiTrust Source*, 2012, 8.

[97] Alex Wilhelm, "White House Drops 'Consumer Privacy Bill Of Rights Act' Draft," *TechCrunch*, February 27, 2015, http://techcrunch.com/2015/02/27/white-house-drops-consumer-privacy-bill-of-rights-act-draft/.

comprehensive online privacy bill — even when Democrats were in charge of Congress. Internet and advertising firms have lobbied heavily against new rules that would interfere with their business models, while Republicans have balked at any government regulation of the Internet, especially from the FTC."[98] In this era of partisanship and gridlock, it is uniquely hard to imagine bipartisan support for a comprehensive privacy bill. It is more likely that we will continue down our segmented approach to privacy protections. This term, Sen. Robert Menendez (D-NJ) did introduce Senate Bill 547, which would establish a comprehensive privacy framework under the FTC; but it has yet to gained traction and has not passed the Senate.[99] We are more likely to see legislation aimed at specific targets, such as data broker regulation, or data breach notification legislation, than we are to see a comprehensive federal reform of online consumer privacy.

In light of the unlikeliness that Congress will pass a Consumer Privacy Bill of Rights in the immediate future, we need to continue to rely on the FTC to protect consumers. Without increased authority from Congress, the FTC will need to continue regulating data collection practices under the authority provided by Section 5 of the FTC Act. This reality makes *FTC v. Wyndham* all the more important. While the FTC won the initial battle, Wyndham appealed and the case is now before United States Court of Appeals for the Third Circuit. If the court were to rule in Wyndham's favor and rule that the FTC has overstepped their authority under Section 5 to regulate data security measures, consumers would left with no recourse. A decision against the FTC would significantly undermine, or possibly eliminate, the agency's ability to enforce not only data security measures, but also data collection practices under Section 5. The FTC has thus

---

[98] Tony Romm, "White House Preps Expansive Online Privacy Bill," *POLITICO*, January 28, 2015, http://www.politico.com/story/2015/01/online-privacy-bill-white-house-114696.html.
[99] "S.547 — 114th Congress (2015-2016)," *Congress.gov*, February 24, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/547/text.

far relied almost exclusively on its Section 5 authority to protect consumers online, and without this authority there would truly be now enforceable oversight of the data collection practices of private companies.

These issues are not going away. Online privacy discussion needs to be brought to the forefront of policy discussion as technology becomes more integrated into our daily lives. The Apple Watch and other "wearable" devices are increasing the amount and intimacy of the personal information collected. The "Internet of things" – where everyday appliances and machines are connected to the Internet – will also increase the volume and details of information collected about consumers. All of these innovations, and many more that have not even been thought of yet, are going to make our lives easier but we must always remember they come at a cost. That cost is consumer privacy. Until we have an open discussion about the costs and benefits of new technologies, as well as the costs and benefits of privacy regulations, we will continue to allow technology to outpace regulators as well as legislators. In the absence of comprehensive consumer privacy legislation, consumers will need continued reliance on FTC enforcement action, and industry self-regulation. However, we have seen the pitfalls of the status-quo. Any consumer privacy legislation needs to start with consumers. We will continue down the current path of inadequate protections unless consumers stand up and demand action. The problems surrounding new technologies and the conflicts they have with consumer privacy are not going away, they are only going to increase in complexity as technology becomes an ever more essential part of our daily lives. It is up to us, the consumers, to demand increased privacy protections in the face of ever more intrusive technologies. Without a grassroots, populist movement where consumers demand privacy legislation from their elected representatives, we will continue down a path where consumers have no meaningful choice in their own privacy.

This does not have to the case, however. We can change; we simply need to address these issues head on, embrace privacy, pass legislation, and prepare ourselves for the future where an ever increasing amount of personal information will be collected.

Bibliography

"A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority." FTC.gov. July 1, 2008. Accessed October 17, 2014. http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

"About Ghostery." *Ghostery.com*. https://www.ghostery.com/en/about.

Angwin, Julia. "AT&T Stops Using Undeletable Phone Tracking IDs." ProPublica. November 14, 2014. http://www.propublica.org/article/att-stops-using-undeletable-phone-tracking-ids.

Angwin, Julia. "The Web's New Gold Mine: Your Secrets." *WSJ*. July 30, 2010. http://www.wsj.com/articles/SB10001424052748703940904575395073512989404.

Bennett, Steven C. "Regulating Online Behavioral Advertising." *The John Marshal Law Review* 44, no. 4 (2011): 899-962.

Berger, Dustin D. "Balancing Consumer Privacy with Behavioral Targeting." *Santa Clara High Technology Law Journal* 27, no. 1 (2010): 1-60.

Boyles, Jan Lauren, Aaron Smith, and Mary Madden. "Privacy and Data Management on Mobile Devices." Pew Research Center. September 4, 2012. http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

"Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019 White Paper." Cisco.com. February 3, 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html.

Clifford, Stephanie, and Quentin Hardy. "Attention, Shoppers: Store Is Tracking Your Cell." The New York Times. July 14, 2013. http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&_r=0.

Clover, Juli. "AT&T Stops Using 'Perma-Cookies' to Track Customer Web Activity." Mac Rumors. November 14, 2014. http://www.macrumors.com/2014/11/14/att-no-longer-using-perma-cookies/.

Collins, Robert Todd Graham. "The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat." *Georgia Law Review* 44, no. 2 (2010): 545-579.

Davik, Christine Suzanne. "We Know Who You Are and What You Are Made Of: The Illusion of Internet Anonymity and Its Impact on Protection from Genetic Discrimination." *Case Western Reserve Law Review* 64, no. 1 (2013): 17-59.

"Do Not Track: Universal Web Tracking Opt Out." *Do Not Track*. http://donottrack.us/.

"Do Not Track." Electronic Frontier Foundation. https://www.eff.org/issues/do-not-track.

"FTC Approves Final Order Settling Charges Against HTC America Inc." FTC.gov. July 2, 2013. https://www.ftc.gov/news-events/press-releases/2013/07/ftc-approves-final-order-settling-charges-against-htc-america-inc.

"FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information." FTC.gov. June 26, 2012. Accessed February 17, 2015. https://www.ftc.gov/es/node/59806.

Federal Trade Commission. *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, (2009). http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf. (accessed October 1, 2014).

Federal Trade Commission. *Mobile Privacy Disclosures: Building Trust Through Transparency,* (2013). https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. (accessed October 1, 2014).

Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* (2010). https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf, (accessed October 1, 2014).

Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* (2012). https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, (accessed October 1, 2014).

Freeman, Jr., D. Reed, Julie O'Neill, and Kimberly S. Robinson. "Industry Associations Launch Behavioral Advertising Self Regulatory Program Involving Icon." Morrison and Foerster. October 6, 2010. http://media.mofo.com/files/Uploads/Images/101006-Behavioral-Advertising.pdf.

Goldfarb, Avi, and Catherine E. Tucker. "Privacy Regulation and Online Advertising." *Management Science* 57, no. 1 (2011): 57-71.

Hale II, Robert V. "Recent Developments in Mobile Privacy Law and Regulation." *Business Lawyer* 69, no. 1 (2013): 237-43.

Hirsch, Dennis D. "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle University Law Review* 34, no. 439 (2011): 439-80, http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr (accessed October 1, 2014).

Hoffman-Andrews, Jacob. "Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls." Electronic Frontier Foundation. November 3, 2014. https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

Hoofnagle, Chris Jay, Ashkan Soltani, Nathaniel Good, and Mika D. Ayenson. "Behavioral Advertising: The Offer You Cannot Refuse." *Harvard Law and Policy Review* 6, no. 273 (August 2012): 273-96.

Johnson, Lauren. "Does Mobile Marketing Actually Work in the Real World?" AdWeek. November 4, 2014. http://www.adweek.com/news/technology/does-mobile-marketing-actually-work-real-world-161180.

Kaye, Kate. "Ad Industry Groups Intro New Rules for Mobile Data Collection." AdAge.com. July 24, 2013. http://adage.com/article/privacy-and-regulation/ad-industry-groups-intro-rules-mobile-data-collection/243261/.

Lane, Julia, Victoria Stodden, Stefan Bender, and Helen Nissenbaum. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambidge: Cambridge University Press, 2014.

Lenard, Thomas M., and PaulH. Rubin. "The FTC and Privacy: We Don't Need No Stinking Data." *The AntiTrust Source*, 2012, 1-8.

Minch, Dr. Robert P. "Privacy Issues in Location-Aware Mobile Devices." *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 2004, 1-10. http://www.computer.org/csdl/proceedings/hicss/2004/2056/05/205650127b.pdf.

Ohm, Paul. "Branding Privacy." *Minnesota Law Review* 97, no. 907 (2013): 908-89.

Ohn, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57 (2009): 1701-777.

Ohm, Paul. "The Rise and Fall of Invasive ISP Surveillance." *University Of Illinois Law Review* 2009, no. 5 (2009): 1417-1496.

"Our History." *FTC.gov*. Accessed October 17, 2014. http://www.ftc.gov/about-ftc/our-history.

"Privacy Badger." *Electronic Frontier Foundation*. April 24, 2013. https://www.eff.org/privacybadger#social.

"Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Preliminary FTC Staff Report) Response of the Electronic Frontier Foundation." Electronic Frontier Foundation. Accessed April 17, 2015. https://www.eff.org/files/ftccommentseff.pdf.

Romm, Tony. "White House Preps Expansive Online Privacy Bill." POLITICO. January 28, 2015. http://www.politico.com/story/2015/01/online-privacy-bill-white-house-114696.html.

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.

"S.547 — 114th Congress (2015-2016)." Congress.gov. February 24, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/547/text.

Schmierer, Catherine. "Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation." *Richmond Journal of Law and Technology* XVII, no. 4 (2011): 1-57, http://jolt.richmond.edu/v17i4/article13.pdf (accessed October 1, 2014).

Schwartz, John. "Giving the Web a Memory Cost Its Users Privacy." *The New York Times*. September 4, 2001. http://www.nytimes.com/2001/09/0 4/technology/04COOK.html

Smith, Aaron. "Cell Internet Use 2012." Pew Research Centers. June 25, 2012. http://www.pewinternet.org/2012/06/26/cell-internet-use-2012/

Smith, Monica S.. *Internet Privacy: Overview and Pending Legislation* CRS Report No. RL31408. Washington, DC: Congressional Research Service, 2004.

Solove, Daniel J. *Understanding Privacy*. Cambridge, Mass.: Harvard University Press, 2008.

Stevens, Gina Marie. *Online Privacy Protection: Issues and Developments* CRS Report No. RL30322. Washington, DC: Congressional Research Service, 2014.

Stevens, Gina. *Privacy Protections for Personal Information Online* CRS Report No. R41756. Washington, DC: Congressional Research Service, 2011. http://www.fas.org/sgp/crs/misc/R41756.pdf.

Stevens, Gina. *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority* CRS Report No. R43723. Washington, DC: Congressional Research Service, 2014. http://fas.org/sgp/crs/misc/R43723.pdf.

Stone, Deborah A. *Policy Paradox: The Art of Political Decision Making*. Rev. ed. New York, New York: Norton, 2002.

The White House. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* (Washington, D.C.: The White House, 2012). https://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed October 1, 2014).

Thierer, Adam. "The Pursuit of Privacy In a World Where Information Control Is Failing." *Harvard Journal of Law & Public Policy* 36, no. 2 (2013): 409-55.

"Third Circuit Hears Oral Arguments in FTC v. Wyndham." Hunton & Williams. March 5, 2015. Accessed February 17, 2015. https://www.huntonprivacyblog.com/2015/03/05/third-circuit-hears-oral-arguments-ftc-v-wyndham.

"TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program." *FTC.gov*. November 17, 2014. https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.

U.S. Const. Amend. IV.

Wilhelm, Alex. "White House Drops 'Consumer Privacy Bill Of Rights Act' Draft." TechCrunch. February 27, 2015. http://techcrunch.com/2015/02/27/white-house-drops-consumer-privacy-bill-of-rights-act-draft/.

Ybarra, Laura. "The E.U. Model as an Adoptable Approach for U.S. Privacy Laws: A Comparative Analysis of Data Collection Laws in the United Kingdom, Germany, and the United States." *Loyola of Los Angeles International and Comparative Law Review* 34, no. 267 (2011): 267-94.

Yi Chung, Yuen. "Goodbye PII: Contextual Regulations for Online Behavioral Targeting." *Journal of High Technology Law,* no. 2 (2014): 414-450.