The FTC's Privacy Leadership Role in the United States
Keynote Address Before Privacy Laws & Business Conference on
Privacy in a Connected World
Commissioner Julie Brill
July 6, 2015

Good afternoon. Thank you, Stewart, for your introduction. And thank you so much for inviting me to address you today. The problem of how to protect privacy in the digital economy is immediate and of global import. And what better place to grapple with the issue than here at St. John's college, one of the most storied and revered institutions of higher learning in the world? I say *one of* – and not *the* – just in case there are Oxonians – or Trinity College alumni – in the audience. As Voltaire said on his deathbed, when asked to renounce the Devil, "This is no time to be making new enemies."

So in preparing my remarks for today, I planned to focus, in a rigorous and academic manner befitting our setting, on the historical underpinnings of the United States Federal Trade Commission's (FTC), approach to data protection and data security. I wanted to explain how – in this brave new world of Big Data, the Internet of Things, social media, mobile marketplaces, and virtual reality – the FTC acts to protect consumer privacy in a manner that adapts to changing technology yet adheres to bedrock principles of consumer protection – principles our agency has held at its core since its founding, one hundred years ago.

One hundred years ago. That sounded pretty impressive, until it was pointed out to me that construction on the Great Gate through which I entered this morning was finished in 1516. Section 5 of the FTC Act, which gives my agency the legal authority to go after companies that deceive consumers or treat them unfairly[1] – an authority we continue to use today to protect consumers' data online – was added in 1938. I am pretty sure the mattress in my hotel room is older than that.

For those of you celebrating the Magna Carta's 800th anniversary, "history" may seem a grand word to use for my discussion of how the FTC has become the leading consumer protection agency in the United States, and how our long record of consumer protection enforcement, policy development, and education have influenced our work on privacy and data security. But as Winston Churchill said, "Study history, study history. In history lies all the secrets of statecraft." Who am I to defy the British Bulldog on his home turf? Besides, even though when measured in Magna Carta years, the FTC's history is beyond brief, I believe a quick review will give you a better understanding of how the FTC protects privacy and where I would like to see the agency's efforts go in the future.

The Consumer Protection Foundations of FTC Privacy Enforcement

The FTC derives its authority to protect consumers from an amendment to the FTC Act, so-called "Section 5," enacted a couple of years before Churchill first became prime minister. Section 5 gives the FTC broad authority to provide remedies for consumers harmed by deceptive

[1] 15 U.S.C. § 45(a).

or unfair practices in the market place. It is a flexible statute that grants the FTC consumer protection authority that changes as technologies and business practices change – an authority that dates from the days of newspaper and radio advertising but serves equally well in the era of connected devices, mobile payments and facial recognition.

To protect consumers from deception, the FTC had long held that it would presume a company's express representations to consumers, as well as certain implied representations, about a good or service are material to consumers' decisions about whether to use it. We have brought hundreds of cases against companies for making deceptive claims in advertising. We have shut down scams that falsely promise to deliver credit repair, mortgage relief, business opportunities, and other services that predominantly target vulnerable consumers. And we have been a leader in stopping robocalls and abusive telemarketing practices.

As consumers spend more and more time in the online marketplace, the FTC has moved its efforts to protect consumers there as well,[2] a migration apparent from a brief look at our work on online companies' privacy policies. Consumers want to know what information they are feeding to online services and what happens to the information once a company has it. This is the purpose that privacy policies serve – or should serve. So it is essential that privacy policies provide information that is true and not misleading. The same goes for disclosures outside of privacy policies, such as in user interfaces.[3] The FTC's deception authority is a vital enforcement tool as consumers move to mobile platforms, connected devices, and beyond.

The FTC had also fleshed out Section 5's consumer protections against unfairness long before we all became surgically attached to our smart phones. The FTC's unfairness standard prohibits acts or practices that cause substantial injury to consumers that they cannot avoid and are not outweighed by benefits to consumers or competition.[4] Importantly, unfairness cases usually do not depend on the representations that companies make to consumers.

Using our deception and unfairness authority under Section 5, we have brought cases and entered into privacy and data security settlements with some of the largest companies in the world, including Google, Facebook, Twitter, and Snapchat,[5] as well as small companies that may

---

[2] For early examples of the application of Section 5 deception authority to privacy policies, see, e.g., *GeoCities, Inc.*, 127 F.T.C. 94 (1999) (consent order) (settling charges that website had misrepresented the purposes for which it was collecting personally identifiable information from children and adults), *available at* https://www.ftc.gov/enforcement/cases-proceedings/commission-decision-volumes/volume-127, and *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (consent order) (challenging website's attempts to sell children's personal information, despite a promise in its privacy policy that such information would never be disclosed).

[3] *See, e.g.*, Facebook, Inc., No. C-4365 (F.T.C. July 27, 2012) ¶¶ 10-18 (complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (alleging that Facebook's privacy settings were deceptive); FTC v. FrostWire LLC, Case No. 11-cv-23643 (S.D. Fla. Oct. 7, 2011) ¶¶ 35-37, *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf (alleging that aspects of a file sharing application's user interface misrepresented the extent to which the files on a consumer's computer would be shared with others).

[5] *See, e.g.*, Snapchat, Inc., C-4501 (F.T.C. Dec. 23, 2014), (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf; Facebook, Inc., C-4365 (F.T.C. July 27,

not be household names. The settlements in these cases – more than 40 of them dealing with privacy, and nearly 60 dealing with data security – have brought greater protections for consumers in the United States, in Europe, and around the world.

In addition to Section 5, the U.S. has numerous privacy laws that apply to specific types of businesses or types of information, and the FTC has a role in enforcing many of them. Laws that protect privacy in healthcare,[6] credit reporting,[7] education,[8] communications,[9] financial institutions,[10] children's information,[11] and other specifically defined sectors or data subjects, along with state laws modeled on the FTC Act, all work alongside Section 5.

The interwoven threads of statutory authority, case law, and, yes, history that backs the FTC's labors to protect consumers and their privacy online presents quite a different picture from the single, unified regulation that the institutions of the European Union are striving to enact. But in terms of practical protections and the privacy values that Europe and the United States protect, we are not too far apart. Just as one would expect of a comprehensive law such as the EU Data Protection Directive,[12] Section 5 has allowed the FTC to address an incredibly wide range of privacy and data security practices. This includes action against mobile apps,[13] social networks,[14] ad networks,[15] purveyors of malware and spyware,[16] and retailers.[17] Section 5 also

---

2012) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf; Google, Inc., C-4336 (F.T.C. Oct. 13, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf; Twitter, Inc. C-4316 (F.T.C. Mar. 2, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf.

[6] Health Insurance Portability and Accountability Act, Pub. L. No.104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

[7] 15 U.S.C. § 1681 *et seq.*

[8] 20 U.S.C. § 1232g.

[9] *See, e.g.*, 47 U.S.C. §§ 222, 338 & 551.

[10] 15 U.S.C. §§ 6801-09.

[11] 15 U.S.C. §§ 6501-06.

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free movement of Such Data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[13] *See, e.g.*, Goldenshores Techs. LLC C-4466 (F.T.C. Mar. 31, 2014) (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf; Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), (decision and order), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.

[14] *See, e.g.*, Facebook, Inc., C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf; Google, Inc., C-4336 (F.T.C. Oct. 13, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

[15] *See, e.g.*, *Chitika, Inc.*, C-4324 (F.T.C. June 7, 2011) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikado.pdf.

provides the basis for the FTC's Safe Harbor enforcement and so plays a pivotal role in sustaining a program that is central to data flows between Europe and the United States.

The Data-Driven Economy and Section 5

Let me turn now to how we meet the privacy challenges posed by the Internet of Things. More and more businesses rely on the data consumers shed whenever they go online, and more and more devices – everything from our refrigerators to our raincoats to our pacemakers – are connected and generating data – often sensitive data.

The new and powerful analytical tools used to parse this data hold tremendous promise. They can help us solve major challenges in healthcare, education, energy use, and other areas. And consumers will reap new benefits and conveniences from barbeque grills that signal when to flip the meat, baby bottles that ensure infants receive adequate nutrition, connected cars that bring more mobility to the disabled, thermostats that save energy, and connected medical devices – and even connected pharmaceutical pills – that save lives.

But connected cars, pills, and cities – and the data that they collect – bring risks, too, especially to consumer privacy. They will collect information about our health conditions and other sensitive traits. They will make available a huge amount of data that can be used to infer what cannot be observed directly. And as sensors become ubiquitous and user interfaces disappear, ensuring that this data collection will take place with consumers' knowledge and consent becomes much more challenging.

The FTC Act can protect consumers when data collection from the Internet of Things crosses the line into deception or unfairness. Two of our recent cases demonstrate this. In one case, the FTC entered into a settlement with a rent-to-own company to resolve our concerns that the company helped its franchisees install and use privacy-invasive software on laptops that consumers rented.[18] The main purpose of this software was to allow franchisees to disable a computer remotely if the consumer fell behind on her payments. However, it also had a "Detective Mode," which allowed franchisees surreptitiously to activate the computer's webcam. As the Commission alleged in its complaint, "[w]ebcams operating secretly inside computer users' homes took photographs of computer users and anyone else within view of the camera."[19] The Commission made clear that collecting such sensitive images in this manner was a source of "actual consumer harm"[20] and unfair.

---

[16] *See, e.g.*, FTC v. CyberSpy Software, LLC, *et al*., No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), (stipulated final order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100602cyberspystip.pdf.

[17] *See, e.g.*, Sears Holdings Mgmt. Corp., C-4264 (F.T.C. Aug. 31, 2009) (decision and order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searsdo.pdf.

[18] *See* FTC, Press Release, Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees (Oct. 22, 2013), *available at* https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer.

[19] Aaron's, Inc., Case No. 4442 (F.T.C. Mar. 10, 2014), at ¶ 5 (complaint), *available at* https://www.ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf.

[20] *Id.* ¶ 16.

The second case involves Internet-connected video cameras. Though widely regarded as being about data security, this case serves as a living example of the adage that "there is no privacy without security." The webcams at issue in this case were vulnerable to a remote hack that led to some 700 video feeds, which included "infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities," being hijacked and posted to a publicly accessible website.[21]

Together these cases show that the FTC Act's prohibitions apply to a wide range of privacy harms, and that the Act gives the FTC the flexibility to enforce some privacy rights of consumers who may not even be aware that data is being collected from them.

Protecting Consumers from Harmful Uses of Big Data

In addition to addressing the practices of companies that collect data directly from consumers through sensors and other connected devices, the FTC is focusing on the vast, mostly invisible network of firms that combine data from consumers' laptops, smartphones, and connected devices with offline material like driving records, mortgage liens, and tax assessments. These companies, known as data brokers, sell a seemingly endless array of information about consumers: what they buy, where they live, how much money they spend, and on what. Some of this information is mundane, particularly when viewed in isolation. But when parsed, combined, and analyzed by sophisticated data brokers, innocent bytes of consumer data become megabytes of detailed personal profiles. And these profiles can include surprisingly sensitive information about a consumer's financial status, race, sexual orientation, and health conditions.

When data brokers fail to keep financial information secure, they create serious risks for consumers. For example, last year the FTC sued two debt brokers for allowing free downloads of files containing sensitive financial information, including bank account numbers, from tens of thousands of consumers.[22] In another case, the FTC took action against a company that sold information about consumers who applied for payday loans. [23] We believe the vast majority of the information was bought by non-lenders, including some who used it to commit fraud.[24]

---

[21] *See* TRENDnet, Inc., No. C-4426 (F.T.C. Jan. 16, 2014) Complaint ¶ 10, *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf,

[22] *See* FTC v. Bayview Solutions, LLC, Case 1:14-cv-01830-RC (D.D.C. Oct. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf *and* FTC v. Cornerstone and Co., LLC, Case 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf. The court in both cases has entered final orders against the defendants. *See* https://www.ftc.gov/system/files/documents/cases/150421bayviewstip.pdf (Bayview final order) *and* https://www.ftc.gov/system/files/documents/cases/150421cornerstonestip.pdf (Cornerstone final order).

[23] FTC v. Sitesearch Corp., d/b/a LeapLab (D. Az. Dec. 23, 2014) (complaint), *available at* http://www.ftc.gov/systems/files/documents/cases/141223leaplabcmpt.pdf.

[24] *Id.* ¶¶ 19-23.

These cases demonstrate clearly how data brokers' violations of consumer privacy can create real harm, and how appropriate it is for the FTC to pursue the violators with our consumer protection jurisdiction. And we have not stopped with enforcement activities. A year ago, the FTC took a deep look at this industry and published its findings and recommendations.[25] We found that data brokers put consumers into "segments" that track sensitive characteristics, including race, religion, ethnicity, sexual orientation, income, and health conditions. I see a clear potential for these profiles to harm low-income and other vulnerable consumers. I fully support the Commission's call for data broker legislation that would bring more transparency, accountability, and consumer control to the data broker ecosystem.

Developing Policies and Best Practices for a Data-Driven World

Our data broker report and recommendations are an example of how the FTC looks beyond enforcement to protect consumers in the data-driven economy. An important part of our consumer protection work is to identify challenges as they emerge, put them up for discussion through public comments and workshops, and recommend practices that will help companies maintain consumers' trust and stay on the right side of the law.

We held a day-long workshop, accepted public comments, and issued a report on the Internet of Things[26]. We also hosted public seminars on user generated health information[27] and retail mobile location tracking.[28] We have also been studying alternative scoring mechanisms that report on individuals based on where they live, their social media interactions, and other nontraditional techniques.[29] In November, the FTC will host a workshop on cross-device tracking, which will begin to explore companies' efforts to tie consumers' behavior across their many different devices.[30]

In all of these examinations, including our report on the Internet of Things, the FTC has repeatedly held that appropriate privacy and data security protections are essential to building consumer trust in connected devices, the companies that provide them, and those that use data from them. This trust has to begin with security. A study released by Hewlett-Packard last year

---

[25] FTC, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 49-54 (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [DATA BROKER REPORT].

[26] FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 29-46 (staff report) (2015), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [IOT REPORT].

[27] FTC, Press Release, Spring Privacy Series: Consumer Generated and Controlled Health Data (May 7, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

[28] FTC, Press Release, Spring Privacy Series: Mobile Device Tracking (Feb. 19, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking.

[29] FTC, Press Release, Spring Privacy Series: Alternative Scoring Products (Mar. 19, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/03/spring-privacy-series-alternative-scoring-products.

[30] FTC, Press Release, Cross-Device Tracking, *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking (last visited June 30, 2015).

found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[31] The FTC is recommending a "security by design" approach that incorporates security into the entire lifecycle of products and services,[32] and we are engaging developers big and small in this ongoing conversation.[33]

Privacy protections will also play an integral role in building consumer trust in the Internet of Things. Our report emphasizes that companies should ask not *whether* Fair Information Practice Principles like notice, choice, and data minimization apply to the Internet of Things, but *how* they apply. This is a challenge. Not only are user interfaces shrinking, but as Erick Schmidt has said, the Internet itself will "disappear".[34] Connectivity will morph into a condition that consumers only notice when it isn't on, like electricity. I believe we need to explore using newly emerging "command centers" for connected home appliances, and other immersive portals and apps, to serve as platforms for consumers to manage the data flows from their connected products and give them meaningful choices about how their private data is handled. But that is just one idea. What is needed most is for companies to unleash their talented designers and engineers to develop creative means for connected products to adhere to Fair Information Practice Principles.

This focus on applying longstanding privacy and data security principles to new technologies and business practices leads to a question that has been vigorously discussed in Washington, in Silicon Valley, and elsewhere in the United States: Should rights and obligations based on the Fair Information Practice Principles be incorporated into a baseline privacy law in the U.S.? My answer is "yes." An appropriate baseline privacy law would accomplish two useful goals: it would create strong, specific, and enforceable protections for consumers, and it would set out clearer rules of the road for businesses, especially when dealing with sensitive information. The discussion draft that the Obama Administration released earlier this year[35] didn't provide these strong, bottom-line protections, but the draft started an important conversation about what baseline privacy legislation in the U.S. should look like. It is a conversation that needs to continue.

That said, I don't believe baseline privacy legislation is enough. I would like to see both data broker legislation and data security legislation also enacted in the U.S. With respect to data

---

[31] Hewlett-Packard, *Internet of Things Research Study* 2 (July 2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

[32] *See* FTC, Careful Connections: Building Security in the Internet of Things (Jan. 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things *and* FTC, Mobile App Developers: Start with Security (Feb. 2013), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security.

[33] FTC, Press Release, FTC Kicks Off "Start With Security" Business Education Initiative (June 30, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.

[34] *See* Chris Matyszczyck, *The Internet Will Vanish, Says Google's Eric Schmidt*, CNET (Jan. 22, 2015, 6:00 PM), *available at* http://www.cnet.com/news/the-internet-will-vanish-says-googles-schmidt/.

[35] Administration Discussion Draft – Consumer Privacy Bill of Rights Act of 2015, *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (last visited July 7, 2015).

security, legislation that supplements the FTC's current "reasonable security" standard with FTC rulemaking and civil penalty authority would put the FTC in a stronger position to hold accountable those companies that fail to take the necessary steps to protect the data that consumers have entrusted to them.

* * * * * *

To sum up, let me return for a moment to Winston Churchill. He said: "History will be kind to me for I intend to write it." While the FTC has been true to our history of protecting consumers and their privacy as our world has moved into the Internet age and beyond, we are also aware we are writing the history for future generations of consumers for whom "online" will become synonymous with "alive." We strive today to make sure the consumers of tomorrow are protected in the cyber-marketplace from unfair and deceptive practices – by encouraging companies to design privacy and security protections into the fabric of their connected products and to ensure consumers have control over their most private data. And if we succeed, I do believe, like Churchill, history will be kind – to the FTC and to the consumers for whom we work.