The Intersection of Privacy and Consumer Protection:
Some Thoughts from FTC Commissioner Julie Brill

U.S. Federal Trade Commissioner Julie Brill
International Consumer Protection and Enforcement Network (ICPEN) Conference
Åre, Sweden (delivered via video)
April 15, 2015

Good afternoon ICPEN! It's been a while since I last spoke with you at the Antwerp meeting, and I am so pleased that I have another opportunity to participate in an ICPEN conference.

The Swedish ICPEN Presidency asked me to focus my talk today on the connection between privacy and consumer protection – a connection that resonates particularly strongly at the U.S. Federal Trade Commission (FTC).

As many of you know, the FTC has a dual mission: to protect consumers and promote competition.[1] We are not a traditional data protection regulator, as exist in many of your countries. Yet the FTC has become one of the leading privacy enforcement agencies in the United States. Our privacy enforcement and policy roles have grown out of our consumer protection mission. The FTC's privacy work protects fundamental privacy values and urges companies to respect these values as technologies and business models change. A strong current running through many of the FTC's privacy enforcement actions is that privacy violations are often linked to a variety other harms, such as deceptive financial practices and fraud, which are often the province of consumer protection regulators. This current is growing stronger.

Before I go much further, I want to make clear that I am not touting the FTC's structure – a single agency that serves as both a privacy regulator and a consumer protection regulator – as a model for other countries to adopt and incorporate into their systems. Instead, I want to focus on issues that you can explore within your country's current framework, in which you serve as your country's leading consumer protection agency, and another entity focuses on data protection. As I describe the connections that we at the FTC are seeing between privacy, the many players in the complex marketplace for personal data – including data brokers, data analytics companies, lead generators, payday lenders, and debt collectors – and a broad array of consumer harms, I think you'll see that these connections are equally deserving of your attention as consumer protection enforcers.

First, let me provide just a bit of background on how some of the laws in the U.S. are designed to address both privacy and consumer protection issues. The Fair Credit Reporting Act[2] (FCRA) governs the uses of credit reports, which were developed as a way to help lenders decide whether specific consumers are worthy of credit. Many of the FCRA's provisions are intended to help ensure that credit reports – and the credit, employment, housing, and other

[1] *See* 15 U.S.C. § 45(a)(2) (granting the FTC the authority to prevent "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce").

[2] 15 U.S.C. § 1681 *et seq.*

major decisions that are based on them – are accurate. The information in credit reports is also deeply personal, so the FCRA limits how companies can use credit reports and provides other protections that follow the Fair Information Practice Principles.[3] Among other things, these comprehensive protections allow consumers to know when information is being used to make important decisions about them and to correct the information when it is inaccurate.

The Fair Debt Collection Practices Act[4] similarly falls at the intersection of privacy and consumer protection concerns. It limits how and when a debt collector may contact consumers, as well as restricting debt collectors from revealing the existence of a debt to third parties. The main purpose of the Fair Debt Collection Practices Act is to prevent debt collectors from using abusive or fraudulent tactics to make consumers pay debts. But it is also a privacy law because it limits the circumstances under which the existence of a debt, which may be deeply embarrassing to a consumer or threaten her employment, may be revealed.

Still other laws protect particularly sensitive information or information about particularly vulnerable consumers. For example, the Children's Online Privacy Protection Act[5] restricts the online collection of information from children. The Gramm-Leach-Bliley Act[6] and its implementing regulations restrict the sharing of personal information by financial institutions and require them to keep consumers' information secure. And the Health Insurance Portability and Accountability Act[7] (HIPAA) protects health information in the hands of health care providers, insurers, and their business associates.

In addition to these laws, which are focused on specific industries and groups of consumers, the FTC uses its authority under Section 5 of the FTC Act[8] to prevent unfair or deceptive acts or practices in privacy and data security cases. Section 5 is a broad, flexible, and remedial statute that allows our enforcement to keep up with changing technologies and business practices. When companies mislead consumers in a material way about their data practices, we use our deception authority. When a company's data practices harm consumers in a way consumers cannot avoid, with no offsetting benefit to consumers or competition, we use our unfairness authority. The FTC has brought and settled actions under Section 5 against companies that are household names in all parts of the world, including Google[9] and Facebook[10],

---

[3] For a general overview of the Fair Information Practice Principles, see FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 19-20 (2015) (staff report), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing views of workshop participants) [IOT REPORT].

[4] *See* Fair Debt Collection Practices Act, 15 U.S.C. § 1692 *et seq.* (associating abusive debt collection practices with "personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy").

[5] 15 U.S.C. § 6801 *et seq. and* COPPA Rule, 16 C.F.R. Part 312.

[6] 15 U.S.C. § 6801 *et seq. and* Safeguards Rule, 16 C.F.R. Part 314.

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

[8] *See generally* 15 U.S.C. § 45.

[9] Google Inc., No. C-4336 (F.T.C. Oct. 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf; United States v. Google Inc., No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012), *available at*

as well as many small companies that engaged in problematic practices. We address practices in a technologically neutral way, focusing on mobile apps[11] and the Internet of Things[12] as well as the Internet of PCs and laptops. Section 5 combined with the sector-specific laws that I discussed provides a good privacy framework in the U.S., although I believe our Congress should act to make it even stronger.

In order to understand the connection between data collection and use practices and your work as consumer protection regulators, we have to look behind the statements that companies make in their privacy policies and beyond the data practices that eventually become evident to consumers and enforcers. Behind the scenes, invisible to consumers and ordinary observers, vast amounts of data about consumers are flowing from their laptops, smartphones, connected devices – and from offline sources like driving records, mortgage liens, and tax assessments – to create detailed, individual profiles. These profiles contain a seemingly endless array of information about consumers: what they buy, where they live, how much money they spend on a specific occasion. Some of this information is mundane when viewed in isolation. But some of the information can be more disconcerting, and certainly more sensitive, such as information about a consumer's financial status, race, sexual orientation, and health conditions. Data brokers and data analytics firms combine all of these data points into comprehensive profiles that create highly revealing pictures about each of us.

I believe that as consumer protection enforcers, we should all be focused on how this data can be used in a manner that harms consumers. Let me focus on the financial arena. In a report that the FTC issued last year,[13] we documented that data brokers collect a wide range of financial information about consumers, and some segment consumers into groups of the "Financially Challenged" or "Modest Wages."[14] This information could help banks find low-income consumers and offer them safe, low-cost financial products. But the same information could be used to target these same consumers with offers for high-cost loans and other products that leave them in worse shape financially. I have long called for data brokers to give consumers more control over the information that goes into marketing profiles and the uses of these profiles, and to be more accountable for how these profiles are used – and misused – by their customers. The FTC and the White House have adopted many of my recommendations.

---

https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf (accepting payment of $22.5 million civil penalty to settle charges that Google violated FTC consent order).

[10] Facebook, Inc., C-4365 (F.T.C. July 27, 2012) (decision and order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[11] *See, e.g.*, Goldenshores Techs., LLC, C-4466 (F.T.C. Mar. 31, 2014) ¶¶ 11-12 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140409goldenshorescmpt.pdf.; United States v. Path, Inc., No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (consent decree and order), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf;

[12] TRENDNet, Inc., No. C-4426 (F.T.C. Feb. 7, 2014), at ¶ 8 (complaint), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

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

[14] *Id.* at 20 n.52.

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 posting files containing information about tens of thousands of consumers on publicly accessible websites, free for anyone to download.[15] These files not only listed debtors by name – and thus revealed who has unpaid debts, a fact that can be sensitive on its own[16] – but also contained full bank account numbers and other sensitive financial information. The Commission believed that this was an unfair disclosure of consumers' information and recently settled actions against the debt brokers.[17]

Lead generators are another set of important players in the market for personal, sensitive information, and their activities can cause concrete and immediate harm to consumers. For example, the FTC recently took action against a "lead generator" that collected information about consumers who were interested in payday loans.[18] The Commission alleged that the company sold information about consumers who applied for payday loans to anyone who wanted to buy it. We believe the vast majority of information went to non-lenders, including some who used the information to commit fraud.[19] We alleged that these disclosures were unfair – and illegal.

Finally, the abundance of information that's available about consumers and their finances can help make a variety of financial scams more convincing and ultimately more damaging to consumers. One of the most common complaints that the FTC receives from consumers is about debt collectors, including so-called "phantom debt collectors," who demand that consumers pay debt that they don't actually owe. By adding personal details in their fraudulent telemarketing schemes, including portions of a Social Security Number, the name of a store where a consumer owed money, or the amount of an old, paid-off debt, phantom debt collectors make their demands much more convincing. Or the scammers might simply find out about a consumer's debt and demand payment, even though the scammer has no right to the payment. The FTC has taken several actions against phantom debt collectors, including one we announced just last week jointly with our partners in the Illinois Attorney General's office.[20]

---

[15] *See* FTC v. Bayview Solutions, LLC, Case 1:14-cv-01830-RC (D.D.C. Aug. 27, 2014), *available at* http://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* http://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf.

[16] *See* Fair Debt Collection Practices Act, 15 U.S.C. § 1692 *et seq.* (associating abusive debt collection practices with "personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy").

[17] FTC v. Bayview Solutions, LLC, Case 1:14-cv-01830-RC (D.D.C. Apr. 13, 2015) (stipulated final order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226/bayview-solutions-llc *and* FTC v. Cornerstone and Co., LLC, Case 1:14-cv-01479-RC (D.D.C. Apr. 13, 2015) (stipulated final order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211/cornerstone-company-llc.

[18] 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.

[19] *Id.* ¶¶ 19-23.

[20] *See* FTC, Press Release, FTC, Illinois Attorney General Halt Chicago Area Operation Charged With Illegally Pressuring Consumers to Pay 'Phantom' Debts (Apr. 10, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/04/ftc-illinois-attorney-general-halt-chicago-area-operation-charged.

Other imposters are using the same techniques – obtaining sensitive and personal financial information about consumers to convince consumers that a fraudulent call is real. We have seen a dramatic rise in complaints about imposters who claim to be from the Internal Revenue Service or other government agencies. Their conversations with consumers are laced with the consumer's Social Security Numbers and other personal information, thereby convincing the consumer that the call is legitimate, and she needs to comply with the caller's demand to pay immediate or else face wage garnishment or arrest. I will be testifying later today at a hearing later today in the U.S. Senate on IRS Imposter Scams and Tax ID theft today.

These misuses of financial information give particularly vivid illustrations of the harms consumers face from data breaches and inadequate accountability regarding data brokers and lead generators. But there are other risks beyond financial harms. Where there is money to be made from using consumers' email addresses, health and medical information, or Web browsing habits, the FTC has found and continues to find companies that are willing to step across legal lines to do so.

The message that I hope you will take away from this discussion is that many of the consumer protection challenges of a data-driven economy go beyond privacy and data protection. While big data and new information infrastructures, such as mobile broadband systems, offer many benefits to consumers – and promise even more – these benefits will be realized only if we enforce safeguards for privacy and data security as well as safeguards against financial fraud and other consumer harms.

Equally, it will be also difficult to fully address these challenges as consumer protection issues without considering the privacy dimensions. These types of challenges are relevant to all of us – whether we are from technologically advanced countries, such as Sweden, Estonia or Japan, or developing countries, where rapidly developing systems of credit reporting and the data-rich mobile banking platforms will bring these issues front and center, perhaps even sooner than you expect.

Let me say a little about our priorities in the coming year in the United States. As I mentioned earlier, I believe U.S. privacy protections are good but should be made stronger. The FTC has consistently called for new federal legislation to address various privacy and data security issues, including data security legislation and legislation governing data brokers. Recently, the Administration released a baseline privacy legislation discussion draft. The release of the proposal is a good step, but I believe any privacy legislation in the U.S. needs to provide clearer bottom-line protections for consumers. I look forward to working with the U.S. Congress and stakeholders from the consumer advocacy community and the private sector to develop them.

The FTC will continue to engage in discussions with a wide variety of stakeholders to inform its policy initiatives. This includes academics, companies, and advocates, as well as our data protection and consumer protection enforcement colleagues around the world. We will continue to hold workshops on cutting-edge issues. Just this past year, the FTC held workshops on mobile security, the Internet of Things, health information generated and controlled by

consumers, and big data and discrimination. In November, we will hold a workshop that examines practices that allow companies to track consumers across the different devices that they use. In addition, the FTC is building its own capacity to analyze and understand new technologies. For the past several years we have had a chief technologist who brings an outside perspective from the technological community. We recently announced the formation of the Office of Technology Research and Investigation, which will provide a larger platform to build our technical expertise. Together, all of these perspectives not only help keep the FTC informed but also provide a forum for different stakeholders to debate and discuss consumer protection challenges.

ICPEN plays a crucial role in providing more cops on the consumer protection beat, and that is needed now more than ever. By sharing our collective knowledge here in ICPEN, we can work together to better protect consumers in a data-driven, global economy. Thank you.