Federal Trade Commission

The FTC's Privacy Program – 2015 and Beyond

Jessica Rich
Director, Bureau of Consumer Protection, FTC

Maastricht University Campus Brussels – October 21, 2015

Good morning. I'm delighted to be here this morning to discuss the important topic of consumer privacy. My plan this morning is to put Safe Harbor aside (if that's even possible) and simply talk about the Federal Trade Commission's privacy and data security program – the laws we enforce, our priorities, and all of the enforcement and policy work we are undertaking.

For those of you who are skeptics about the US approach to privacy – and I think there are many here – I hope to at least *surprise* you with the breadth and depth of our efforts and accomplishments in this important area. For over two decades, the FTC has made privacy one of its top priorities. During this time, we've have brought hundreds of privacy enforcement actions addressing a wide range of practices across the economy, hosted many dozens of workshops, written scores of reports, and issued millions of consumer and business educational materials.[1]

With the rapid growth of technology in recent years, privacy has become an ever more prominent part of the FTC's work. Indeed, technology has changed the global marketplace as we've known it. The surge in the use of smartphones and connected devices provides consumers with an incredible variety of goods, services, conveniences, and experiences that they have come to expect. From wherever they are, they can find information, contact friends, shop and pay for goods and services, update their social networks, monitor their health and fitness, and access devices in their cars and homes remotely.

But these changes also pose immense challenges for consumer privacy. Today, data is collected from consumers wherever they go – online, offline, through mobile and connected devices, everywhere. Most of the companies that collect consumers' data are behind the scenes, completely unknown to consumers. The plunging costs of data storage and processing mean that companies are keeping data for longer and using it in many new ways and for many purposes. And this trend toward ubiquitous and invisible data collection and use will only accelerate as we move further into the era of Big Data and the Internet of Things.

The consequences for consumers are very serious and very real: massive collection and storage of personal information; the risk that detailed profiles will fall into the wrong hands, enabling identity theft and other harms; the release or exposure of sensitive information consumers regard as private; and the potential use of personal data by employers, insurers, creditors, and others to make important decisions about consumers.

The FTC's privacy program seeks to address these concerns through law enforcement, policy initiatives, and education. Many of our efforts are guided by three basic principles that build on the long-established fair information practices. First is Privacy by Design – build meaningful privacy and data security protections into your business model from the very start. Don't add them afterwards as an afterthought. Second is Transparency – tell consumers how you will collect, use, and share their data. But don't just tell them in a privacy policy; provide them with important information at the moment of a transaction or in some other prominent place where can see and act on it. Third is Choice – give consumers choices about any collection, use, and sharing that isn't obvious or implied from the context, and provide opt-in choice whenever sensitive data is involved.

I. FTC Jurisdiction and Authority

Before I tell you about our specific initiatives, I'd like to provide a little background for those of you who aren't familiar with the Commission. The FTC has broad jurisdiction over most entities engaged in commerce – just not banks and few other exceptions. Our primary authority is the FTC Act, which prohibits unfair and deceptive trade practices.[2] The basic rules are that companies can't deceive consumer or engage in practices that cause substantial consumer injury without countervailing benefits to consumers or competition. The FTC Act is flexible by design, and we've used our authority to challenge a very wide range of practices. False claims and material omissions about how data will be used or shared. Failure to provide reasonable security protections for consumer data. Invisible spyware that infects consumers computers or

steals their information. Invasive and unwanted spam. Impersonating consumers in calls to financial institutions, in order to obtain their data. Posting consumers' sensitive data online and then seeking money from the consumers to take it down. Tricking consumers into consenting to certain data practices. Capturing people's private communications and photos through tracking software. Selling data that is then used for fraud. Etcetera.

The Commission also enforces a number of sector-specific privacy laws. These include the Fair Credit Reporting Act, which protects the privacy and accuracy of sensitive consumer report information;[3] the Gramm-Leach-Bliley Act, which imposes privacy and security requirements on non-bank financial institutions;[4] the Children's Online Privacy Protection Act;[5] the CAN-SPAM Act;[6] and the Telemarketing and Consumer Fraud and Abuse Prevention Act[7] with its Do Not Call Rule.[8]

In addition, the FTC educates consumers and businesses, conducts studies, testifies before Congress, hosts workshops, and writes reports regarding the privacy and security implications of technologies and business practices that affect consumers. We issue educational materials on a wide range of topics – from mobile device security to kids' online safety to preventing and repairing identity theft, our top source of consumer complaints from year-to-year. Our outreach efforts are designed to prevent law violations and harm before they happen, and are therefore integral to our mission.

We are not the only US agency working on privacy and data security issues. A variety of other federal agencies, such as the Federal Communications Commission and the Consumer Financial Protection Bureau, have privacy authority in specific sectors. And many of the US States also have robust privacy laws and active enforcement

programs. The FTC, however, has the broadest jurisdiction, which we have used aggressively over the past two decades, and we intend to continue to lead the US' privacy enforcement and policy efforts as we move forward.

II. Recent Cases and Policy Initiatives

Our recent initiatives in the privacy area illustrate the breadth and volume of our privacy enforcement and policy work. For example, last year, we brought a multiple-count action against mobile messaging app Snapchat for privacy and security violations. Among other things, Snapchat had promised that the photos and videos sent through its app would disappear at a time set by the sender.[9] In fact, we alleged that recipients could use easy workarounds to keep the messages forever.

We also took action against the maker of a popular flashlight app for misrepresenting that it would only collect data from users' devices for certain internal housekeeping purposes. [10] In fact, we alleged that it collected – and transmitted to third party ad networks – the device's location and device ID. A flashlight app!

More recently, we addressed the growing practice by retailers of using mobile technologies to track the movements of their customers in stores. We alleged that Nomi Technologies, the analytics firm that performed these services, told consumers they would be notified when stores were using its tracking services and would be able to opt out then and there.[11] In fact, consumers weren't told at stores and couldn't opt out at stores.

Health data is another important FTC concern because it's sensitive and often regarded as private. In December, we charged Payments MD, a health billing company,

with using a deceptive registration process to trick thousands of consumers who signed up for its online billing portal into also consenting to the collection of their detailed medical information from pharmacies, medical labs, and insurance companies.[12]

Then there are extortion websites that harvest sensitive data, post it online, and seek payment to take it down. We took action against two of those this year. In one, defendant Craig Brittain solicited sexually explicit photos from women's ex-boyfriends and others – in many cases through deception – to post on his website, isanybodydown.com.[13] He then used another site to pose as an attorney and charge $250 for removing the information. We brought a similar actions against a company called Jerk.com, which posted photos of kids and teens, labeled as a "jerk," supposedly by their peers.[14]

We've also brought numerous actions against companies that failed to implement reasonable protections for sensitive data – indeed, over 50 during the last 15 years.[15] Last year, for example, we brought our first data security action involving the Internet of Things. We alleged that video monitoring company TRENDnet failed to provide reasonable security for IP cameras used for home security and baby monitoring, which resulted in hackers posting private video feeds of people's bedrooms and children's rooms on the Internet.[16]

And we've brought a number of cases involving mobile device security – including against mobile device manufacturer HTC for failing to secure its mobile devices,[17] and against mobile apps Credit Karma[18] and Fandango[19] for disabling a critical default process necessary to ensure that their apps' communications were secure.

Other recent data security cases include actions against service provider Accretive Health,[20] supplement companies Genelink[21] and Genewize,[22] medical transcriber GMR Transcription Services,[23] and debt brokers Bayview[24] and Cornerstone.[25] These cases all involved the failure to secure sensitive information – in some cases health data, in some cases financial data. And we have ongoing litigation against Wyndham Hotels[26] and LabMD[27] – and a contempt action against Lifelock[28] – for alleged failures to protect sensitive financial and health data. In *Wyndham*, the Third Circuit recently reaffirmed the FTC's authority under the FTC Act to hold companies accountable for security failures.

This year, we are emphasizing our data security educational tools and taking our message on the road with our *Start with Security* campaign.[29] It includes events around the country on security topics and best practices. And we continue to put out new business guidance on data security, including our latest piece on lessons learned from the FTC's over 50 data security cases.[30]

Additionally, we are vigorously enforcing the laws protecting children's privacy,[31] sensitive consumer report data, [32] and (until just recently) European citizens' data protected by the Safe Harbor Framework.[33] To date, we've brought 25 cases to enforce the Children's Online Privacy Protection Act (COPPA), including two recent cases against the mobile app for Yelp and the gaming app TinyCo, both of which paid significant penalties.

In the area of consumer reporting, we've brought 100 cases to date, and have obtained over $30 million in civil penalties. In two recent cases, for example, we alleged

that data brokers InfoTrack[34] and Instant Checkmate[35] sold detailed background checks to employers and landlords without ensuring that the data was accurate, or that purchasers had a permissible purpose to buy it, as required by the Fair Credit Reporting Act.

And as of the date of the recent European Court of Justice ruling, we had brought 39 actions to enforce the Safe Harbor Framework, including cases against Google, Facebook, and Myspace. The orders in these actions are not affected by the ruling and will continue to protect the privacy of millions of European residents for years to come.

One theme I am stressing in our privacy program is the connection between the sale of sensitive data and fraud. In fact, I have directed the attorneys that bring our fraud cases to examine whether the defendants in those cases purchased consumer data from other companies to aid in the fraud.

Two recent cases illustrate this troubling problem. Data brokers Leap Lab and Sequoia One both purchased the payday loan applications of financial strapped consumers – which included names, addresses, phone numbers, employers, SSNs, and bank account numbers – and sold them to scam artists who used the data to withdraw millions of dollars from consumers' accounts.[36] The Commission declared the sale of this data to be an unfair practice under the FTC Act.

Finally, in the last two years, the FTC has hosted workshops and released influential reports about trends and privacy concerns in today's marketplace. These include last year's "Spring Privacy Series" to examine mobile device tracking in retail stores,[37] predictive scoring models used for marketing,[38] and health apps and devices,[39] as well as our May 2014 report on data brokers.[40]

In addition, last fall, we hosted a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?*[41] The workshop explored how the categorization of consumers may be both creating and limiting opportunities for consumers, with a focus on low income and underserved consumers. We plan to issue a report on this topic in the coming months. And in January, we issued a staff report recommending best practices for the Internet of Things.[42]

More policy work is in the pipeline. In October, we'll host a workshop to examine the growing use of online lead generation in various industries, including consumer lending and education.[43] The goal is to highlight best practices for entities that generate and sell consumer leads so they can avoid becoming a Leap Lab or Sequoia One, in the crosshairs of the FTC. In November, we'll host a workshop on cross-device tracking to examine the various ways that companies now track consumers across multiple devices, and not just within one device.[44] And in January, we will host a conference called PrivacyCon to examine cutting-edge research and trends in protecting consumer privacy and security.[45]

III. Conclusion

As you can see, the FTC is committed to protecting consumer's privacy in this increasingly digital era. We are using all tools at our disposal to challenge and stop practices that violate consumers' privacy and to prevent violations through outreach and education. I look forward to further discussion during today's panels.

[1] *See, e.g.*, *Privacy and Security Update (2014)* (Jan. 2015), *available at* https://www.ftc.gov/reports/privacy-data-security-update-2014.
[2] 15 U.S.C. § 45(a).
[3] 15 U.S.C. §§ 1681–1681x.
[4] *See* 16 C.F.R. Parts 313 & 314, implementing 15 U.S.C. § 6801(b).
[5] 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312.
[6] 15 U.S.C. §§ 7701-7713; *see also* 16 C.F.R. Part 316.
[7] 15 U.S.C. §§ 6101-6108.
[8] 16 C.F.R. Part 310.
[9] *Snapchat, Inc.*, No. C-4501 (Dec. 23, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter.
[10] *Goldenshores Technologies, LLC*, No. C-4446 (Mar. 31, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter.
[11] *Nomi Technologies, Inc.*, No. C-4538 (Sept. 3, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter.
[12] *PaymentsMD, LLC*, No. C-4505 (Jan. 27, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3088/paymentsmd-llc-matter.
[13] *Craig Brittain*, Matter No. 132-3120 (Jan. 29, 2015) (proposed consent agreement), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter.
[14] *Jerk, LLC*, Docket No. 9361 (Mar. 13, 2015) (summary judgment decision), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3141/jerk-llc-dba-jerkcom-matter.
[15] *See, e.g.*, *Commission Statement Marking the FTC's 50th Data Security Settlement*, Jan. 31, 2014, *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[16] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[17] *HTC America, Inc.*, No. C-4406 (June 25, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.
[18] *Credit Karma, Inc.*, No. C-4480 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc.
[19] *Fandango, LLC*, No. C-4481 (Aug. 13, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc.
[20] *Accretive Health, Inc.*, No. C-4432 (Feb. 5, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter.
[21] *Genelink, Inc.*, No. C-4456 (May 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/genelink-inc-matter.
[22] *foru Int'l Corp.*, No. C-4457 (May 8, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3095/forutm-international-corporation-matter.
[23] *GMR Transcription Servs., Inc.*, No. C-4482 (Aug. 14, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.
[24] *FTC v. Bayview Solutions LLC*, No. 1:14-cv-01830-RC (D.D.C. filed Oct. 31, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc.
[25] *FTC v. Cornerstone & Co.*, No. 1:14-cv-01479-RC (D.D.C. filed Aug. 27, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc.
[26] *FTC v. Wyndham Worldwide Corp.*, Civil No. 13-1887 (ES) (D.N.J. Apr. 7, 2014) (opinion denying defendant's motion to dismiss), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation.

[27] *LabMD Inc.*, Docket No. 9357 (filed Aug. 28, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[28] *FTC v. Lifelock Inc.*, No. 2:10-cv-00530-MHM (D. Az. filed July 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.

[29] *See* 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.

[30] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[31] *See, e.g., U.S. v. Yelp, Inc.*, No. 3:14-cv-04163 (N.D. Cal. filed Sept. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3066/yelp-inc; *U.S. v. TinyCo, Inc.*, No. 3:14-cv-04164 (N.D. Cal. filed Sept. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3209/tinyco-inc.

[32] *U.S. v. Instant Checkmate, Inc.*, No. 3:14-cv-00675-H-JMA (S.D. Cal. Apr. 1, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3221/instant-checkmate-inc; *U.S. v. Infotrack Information Servs., Inc.*, No. 1:14-cv-02054 (N.D. Ill. Mar. 24, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3092/infotrack-information-services-inc-et-al; *U.S. v. Telecheck Servs., Inc.*, No. 1:14-cv-00062 (D.D.C. Jan. 16, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3183/telecheck-services-inc; *U.S. v. Certegy Check Servs., Inc.*, No. 1:13-cv-01247 (D.D.C. Aug. 15, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/112-3184/certegy-check-services-inc.

[33] To date, we have brought almost forty cases against companies that violated the framework, including thirteen this past August. *See* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework.

[34] *U.S. v. Infotrack Information Servs., Inc. et al.*, No. 1:14-cv-02054 (N.D. Ill. Mar. 24, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3092/infotrack-information-services-inc-et-al.

[35] *U.S. v. Instant Checkmate, Inc.*, No. 3:14-cv-00675-H-JMA (C.D. Cal. Apr. 9, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3221/instant-checkmate-inc.

[36] *FTC v. Sitesearch Corp., LLC*, Matter No. 142-3192 (D. Az. filed Dec. 22, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab; *FTC v. Sequoia One, LLC*, No. 2:15-cv-01512-JCM-CWH (D. Nev. filed Aug. 12, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.

[37] FTC Seminar, *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.

[38] FTC Seminar, *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.

[39] FTC Seminar, *Spring Privacy Series: Consumer Generated and Controlled Health Data* (May 7, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data.

[40] FTC Report, *Data Brokers: A Call For Transparency and Accountability* (May 2014), *available at* https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

[41] FTC Workshop, *Big Data: A Tool for Inclusion or Exclusion?* (Sept. 15, 2014), *available at* https://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.

[42] FTC Staff Workshop Report, *The Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.

[43] FTC Workshop, *Follow the Lead: An FTC Workshop on Lead Generation* (Oct. 30, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/10/follow-lead-ftc-workshop-lead-generation.

[44] FTC Workshop, *Cross Device Tracking* (Nov. 16, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

[45] *See* FTC Press Release, *FTC Announces PrivacyCon, Issues Call to Whitehat Researchers and Academics for Presentations* (Aug. 28, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/ftc-announces-privacycon-issues-call-whitehat-researchers.