UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Prepared Remarks of Chairman Joseph Simons[1]
Welcome and Opening Remarks – PrivacyCon 2019
June 27, 2019

Thank you, all, and welcome to PrivacyCon 2019. During my first stint at the FTC in the 1980s, personal computers were just being introduced into our offices and homes. No one imagined that we would soon be carrying them in our pockets, speaking commands to them, or using other devices to track our fitness regimes, unlock our doors, and control our thermostats.

Few of us then envisioned the advances in technology we would experience in our lifetimes, and the effect they would have on our everyday lives. Even fewer of us had the foresight to recognize the commodity unifying these technological advances: our data.

When consumers engage digitally, companies collect information about their choices, experiences, and individual characteristics. Every day, companies make countless decisions based on our likes and dislikes, our relationships and conversations, and our transactions and purchases. They carefully assemble, synthesize, trade, and sell these small bits of data, providing insights into market-wide tastes and emerging trends, and allowing for the prediction of individualized preferences.

No doubt, this vast amalgamation of data has allowed for great technological advances, but it also comes with a certain degree of risk. News stories highlight troubling privacy and data security practices on a regular basis—whether it is allegations of using facial recognition

[1] These remarks reflect my own views. They do not necessarily reflect the views of the Commission or any other individual Commissioner.

technologies and images without users' consent,[2] breaches that expose health data,[3] or sharing genetic data beyond consumers' expectations.[4] These types of privacy and data security "fails" don't just generate headlines: they can cause a range of real harms, including fraudulent charges on credit cards,[5] safety risks,[6] reputational injury,[7] and unwarranted intrusions into people's homes and the intimate details of their lives.[8]

In part to examine these types of incidents and the injuries associated with them, we hosted our first Privacy Con in 2016. Since then, PrivacyCon has been an annual event that has enabled us to advance our consumer protection mission in various ways. It has allowed the FTC to stay up-to-date with emerging technologies. It has helped us to identify potential areas for enforcement and to fashion remedies in our orders. And it has highlighted areas in which we can provide additional business and consumer education.

This is my first PrivacyCon as Chairman. As you undertake your discussions today, I thought it would be useful for you to hear about some of the FTC's current priorities on privacy

---

[2] Russell Brandom, *Microsoft Pulls Open Facial Recognition Dataset after* Financial Times *Investigation*, THE VERGE (June 7, 2019), https://www.theverge.com/2019/6/7/18656800/microsoft-facial-recognition-dataset-removed-privacy.

[3] John Burcham, *Quest Diagnostics Breach Leaks Personal Information for Nearly 12 Million Patients*, FIGHTING IDENTITY CRIMES (June 4, 2019), https://www.fightingidentitycrimes.com/quest-diagnostics-data-breach/.

[4] Eric Ravenscraft, *How to Protect Your DNA Data Before and After Taking an at-Home Test*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html.

[5] Al Pascaul, et al., *2018 Identity Fraud: Fraud Enters a New Era of Complexity*, JAVELIN (Feb. 6, 2018), https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

[6] *FTC v. Accusearch, Inc.*, No. 06-CV-0105 (D. Wyo. May 3, 2006), https://www.ftc.gov/enforcement/casesproceedings/052-3126/accusearch-inc-dba-abikacom-jay-patel (alleging that telephone records pretexting endangered consumers' health and safety); *FTC v. EMP Media, Inc. also d/b/a Myex.com*, No. 2:18-CV-00035 (D. Nev. Jan. 9, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3052/emp-media-inc-myexcom (alleging revenge porn website led to threats and harassment against individuals depicted).

[7] *See, e.g.*, *FTC v. Ruby Corp.*, No. 1:16-CV-02438 (D.D.C. Dec. 14, 2016), ¶ 40, https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (Complaint) (alleging "substantial injury to consumers in the form of . . . disclosure of sensitive, personal information" [membership in infidelity-enabling dating service]).

[8] *See, e.g.*, FTC Press Release, *Aaron's Rent-to-Own Chain Settles FTC Charges That it Enabled Computer Spying by Franchisees* (Oct. 22, 2013), https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chainsettles-ftc-charges-it-enabled-computer; FTC Press Release, *FTC Halts Computer Spying* (Sept. 25, 2012), https://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying.

and security.

First and foremost is vigorous enforcement. Where we have statutory authority, we have used it to the full extent. In the past year, we have brought privacy and security cases under the laws we enforce, and in the limited areas in which we have civil penalty authority, we have used it aggressively. In February, we announced our highest penalty in a children's privacy case, against Tik Tok, a popular video social networking app.[9] Last fall, we obtained a $3 million civil penalty under the Fair Credit Reporting Act against a company whose automated decision-making tool provided inaccurate data to property managers, resulting in denial of housing.[10]

Second, I have been very focused on improving our non-monetary remedies in privacy and security cases, in order to provide better deterrence. As part of our *Hearings on Competition and Consumer Protection in the 21st Century*, we hosted a data security hearing, including a panel focused specifically on the FTC's data security enforcement.[11] Partly in response to feedback we received during the hearing, we have incorporated new provisions in our data security orders. For example, in three recent cases, we required that senior officers provide annual certifications of order compliance to the Commission, thus improving individual accountability.[12] While we continue to require that companies implement a comprehensive, process-based data security program, in our most recent case we also included specific requirements that the company conduct yearly employee training, monitor its systems for data

---

[9] *United States v. Musical.ly, Inc.*, No. 2:19-CV-01439 (C.D. Cal. Feb. 27, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically-inc.

[10] *FTC v. Realpage, Inc.*, No. 3:18-CV-02737 (N.D. Tex. Oct. 16, 2018), https://www.ftc.gov/enforcement/cases-proceedings/152-3059/realpage-inc.

[11] FTC Hearing on Data Security (Dec. 11-12, 2018), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-december-2018.

[12] *James. V. Grago, Jr. also d/b/a ClixSense.com*, Matter No. 1723003 (Apr. 24, 2019) (proposed consent order), https://www.ftc.gov/enforcement/cases-proceedings/172-3003/james-v-grago-jr-doing-business-clixsensecom; *U.S. v. Unixiz, Inc. d/b/a i-Dressup.com et al.*, No. 5:19-cv-02222 (N.D. Cal. Apr. 24, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3002/unixiz-inc-doing-business-i-dressupcom; *LightYear Dealer Technologies, LLC*, FTC Case. No. 1723051 (June 12, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3051/lightyear-dealer-technologies-llc-matter-0.

security incidents, and implement access controls. We also made significant changes to improve the accountability of the third-party assessor that reviews the company's data security program, requiring that the assessor "look under the hood" rather than relying on the company's assertions, and creating greater FTC oversight over the assessor.[13]

Third, we continue to use all of the non-enforcement tools at our disposal to further our privacy and data security mission. For example, we have proposed amendments to the Safeguards Rule to add more detailed requirements.[14] The comment period closes in August. We have used our authority under Section 6(b) of the FTC Act to request information from several U.S. internet broadband providers and related entities to examine how broadband companies collect, retain, use, and disclose information about consumers.[15] Finally, we have engaged in advocacy. Recognizing the limitations of our primary legal enforcement tool, Section 5 of the FTC Act,[16] we have urged Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers.

Which brings us to today. We are using yet another tool at our disposal—PrivacyCon—to continue promoting privacy and data security. Today's program has four sessions that will address a variety of important topics. Our first panel, "Privacy Policies, Disclosures, and Permissions," will explore privacy policies, how data collection aligns with those practices, and

---

[13] *LightYear Dealer Technologies, LLC*, FTC Case. No. 1723051 (June 12, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3051/lightyear-dealer-technologies-llc-matter-0.

[14] FTC Press Release, *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules* (Mar. 5, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules.

[15] FTC Press Release, *FTC Seeks to Examine the Privacy Practices of Broadband Providers* (Mar. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers.

[16] 15 U.S.C. § 45. Section 5 of the FTC Act prohibits unfair and deceptive acts or practices. But it is an imperfect tool. For example, Section 5 does not allow the Commission to seek civil penalties for first-time privacy violations. It does not allow us to reach non-profits and common carriers, even when their practices have serious implications for consumer privacy and data security.

the GDPR's impact on privacy both on the web and on apps. Our second panel, entitled "Consumer Preferences, Expectations, and Behaviors," will examine consumer attitudes toward digital privacy, and take a deeper dive into IoT devices, smart homes, and COPPA. Our third panel, "Tracking and Online Advertising," will consider the commercial impact of tracking technologies, free versus paid apps, and GDPR's effect on e-commerce. Finally, our fourth panel—"Vulnerabilities, Leaks, and Breach Notifications"—will consider the data security aspects of apps and the effectiveness of breach notifications.

I know I am excited to get to the presentations. But before we do, I want to thank everyone who has made this event today possible. First, I want to thank the 19 researchers presenting today and the dozens of co-authors who submitted research for today's event. Thank you to Andi Arias and Jamie Hine for leading the planning of this PrivacyCon. And I also want to thank the many other FTC colleagues from the Division of Privacy and Identity Protection, Bureau of Economics, Division of Consumer and Business Education, Office of Public Affairs, and Office of the Executive Director who have worked together to produce this event. Finally, thank you to everyone who is attending in person or watching online via our live webcast. We appreciate the opportunity to engage the public on these important research endeavors, and I hope you enjoy the FTC's fourth PrivacyCon.