COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

February 22, 2019

To: Subcommittee on Consumer Protection and Commerce Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on Protecting Consumer Privacy in the Era of Big Data

On **Tuesday, February 26, 2019, at 10 a.m. in the John D. Dingell Room, 2123 of the Rayburn House Office Building**, the Subcommittee on Consumer Protection and Commerce will hold a hearing entitled, "Protecting Consumer Privacy in the Era of Big Data."

I. BACKGROUND

In today's global economy, consumer data and information are indispensable. Companies use countless methods and mechanisms to collect, aggregate, analyze, use, and disseminate vast amounts of data about consumers. Reasonable collection and use of consumers' information benefits businesses and consumers. For example, companies must collect information to process transactions and conduct day-to-day operations, such as authentication, fraud prevention, and background checks. In addition, marketing databases help companies identify new sales leads, improve customer service, develop new lines of products, and make marketing more efficient.

At the same time, data collected from consumers has been used for questionable practices. For example, individuals purchased real-time cell phone location data to unknowingly track others such as their girlfriends.[1] In addition, advocates argue that consumer data has been used to discriminate, leading to concerns about access to housing, lending, digital redlining, and voter suppression.[2]

Data collection practices are complex, however, and vary from entity to entity. Even when consumers are given privacy options, there is still little transparency and individual choice. Many of these options may be difficult for consumers to find or to enable and use effectively. They may require the payment of fees, for example, or only partially address the collection or

[1] *I Gave a Bounty Hunter $300. Then He Located Our Phone*, Motherboard (Jan. 8, 2019) (motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile).

[2] The Leadership Conference on Civil and Human Rights, *Address Data-driven Discrimination, Protect Civil Rights* (Feb. 13, 2019) (civilrights.org/resource/address-data-driven-discrimination-protect-civil-rights/).

use of their data and information. In addition, some companies, known as data brokers, who have no direct relationship with consumers, aggregate and monetize consumer data while providing little or no transparency and choice to the individual.

Consumers' privacy concerns have increased over the past several months due to a series of high-profile incidents, including the Cambridge Analytica/Facebook data leak;[3] two bugs in Google+ that allowed third-party app developers to access millions of users' personal information;[4] and an Amazon Alexa that shared a recording of a couple's conversation without permission.[5] Further, data breaches of sensitive information continue at an alarming pace. According to the Privacy Rights Clearinghouse, more than 11 billion records containing sensitive personal information have been involved in security breaches since January 2005.[6]

II. FEDERAL ROLE IN CONSUMER PRIVACY

No federal law comprehensively governs the collection, use, and dissemination of consumer information.[7] Specific federal laws, however, cover certain categories of personal information and specific entities. For example, the Fair Credit Reporting Act (FCRA) governs consumer report information;[8] Title V of the Gramm-Leach-Bliley Act (GLBA) addresses the sharing of certain nonpublic personally identifiable information by financial institutions;[9] and rules issued under the Health Insurance Portability and Accountability Act (HIPAA) apply to the privacy of medical records.[10] In addition, the Children's Online Privacy Protection Act (COPPA) imposes specific requirements, such as obtaining parental consent before collecting

---

[3] *87 Million Facebook Users to Find Out If Their Personal Data Was Breached*, ABC News (Apr. 9, 2018) (abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187).

[4] Electronic Frontier Foundation, *The Google+ Bug Is More About the Cover-Up Than the Crime* (Oct. 11, 2019) (www.eff.org/deeplinks/2018/10/google-bug-more-about-cover-crime); *Google Reveals New Security Bug Affecting More Than 52 Million Users*, Washington Post (Dec. 10, 2018) (www.washingtonpost.com/technology/2018/12/10/google-reveals-new-security-bug-affecting-more-than-million-users/?utm_term=.3499d20fe0c1).

[5] *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation*, New York Times (May 25, 2018) (www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html?rref=collection%2Ftimestopic%2FPrivacy).

[6] Privacy Rights Clearinghouse, *A Chronology of Data Breaches* (www.privacyrights.org/data-breaches) (accessed February 6, 2019).

[7] *See generally* Congressional Research Service, *Information Brokers: Federal and State Laws* (May 5, 2006) (RL-33005); Congressional Research Service, *Privacy Law and Online Advertising: Legal Analysis of Data Gathering by Online Advertisers Such as Double Click and NebuAd* (Feb. 20, 2009) (RL-34693).

[8] 15 U.S.C. § 1681 *et seq.*

[9] 15 U.S.C. §§ 6801-6809.

[10] 45 C.F.R. Part 164.

personal information, on websites and online services directed to children under 13 years old or website operators with actual knowledge that personal information is being collected from children under 13 years old.[11]

The Federal Trade Commission (FTC) may bring actions for unfair and/or deceptive acts or practices under the FTC Act, which includes the authority to bring actions related to a company's collection and use of consumers' information.[12] Unlike FCRA, GLBA and HIPPA, the prohibition on unfair and/or deceptive acts or practices does not impose specific privacy regulations on companies, but it does enable the FTC to take action against companies that fail to live up to affirmative commitments they make.

III. OTHER LAWS

The General Data Protection Regulation (GDPR) went into effect in the European Union (EU) in May 2018. GDPR applies to all companies that hold or process data within the EU.[13] Among other things, it gives consumers certain rights to control the use and disclosure of their information, including a right to access their information, a right to object to processing of their information, and the right to be forgotten.[14] Companies can be fined up to €20 million or four percent of global revenue for GDPR violations.[15] The regulation also includes a private right of action for those affected by a violation, allowing them to obtain compensation from the violator.[16]

In June 2018, California enacted the nation's first comprehensive state consumer privacy statute, known as the California Consumer Privacy Act. The law recognizes and enumerates certain privacy rights and protections for California residents, including the right to know what personal information is being collected about them; the right to know whether their personal information is sold and to whom it is sold; the right to opt out of the sale of their personal information; the right to access the information collected about them; and the right not to be discriminated against for exercising their privacy rights.[17] With some exceptions, California residents may also request deletion of their personal information.[18] California's new privacy statute is enforced by the California Attorney General through civil penalties by the California Attorney General and includes a limited private right of action for data security violations.[19]

---

[11] 15 U.S.C. § 6501 *et seq*.

[12] 15 U.S.C. § 45(a)(2).

[13] General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

[14] *Id*.

[15] *Id*.

[16] *Id*.

[17] Cal. Civil Code § 1798.100 et seq.

[18] *Id*.

[19] *Id*.

III. WITNESSES

Brandi Collins-Dexter
Senior Campaign Director
Media, Democracy & Economic Justice
Color of Change

Dave Grimaldi
Executive Vice President for Public Policy
IAB

Roslyn Layton, PhD
Visiting Scholar
American Enterprise Institute

Nuala O'Connor
President and CEO
Center for Democracy & Technology

Denise Zheng
Vice President, Technology, Innovation
Business Roundtable