United States Government Accountability Office

Testimony

Before the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, March 7, 2019

INTERNET PRIVACY AND DATA SECURITY

Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility

Statement of Alicia Puente Cackley, Director, Financial Markets and Community Investment

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee:

Thank you for the opportunity to testify today about Internet privacy and data security issues. The United States does not have a comprehensive data privacy law at the federal level and instead relies in part on a sectoral approach with industry-specific laws enforced by various agencies governing areas such as healthcare and financial services. In addition, the Federal Trade Commission (FTC) currently has the lead in overseeing Internet privacy across all industries, with some exceptions. Specifically, FTC addresses consumer concerns about Internet privacy using its broad authority to protect consumers from unfair and deceptive trade practices. FTC has jurisdiction over a broad range of entities and activities that are part of the Internet economy, including websites, applications (apps), advertising networks, data brokers, device manufacturers, and others.

My testimony today addresses (1) FTC's role and authorities for overseeing Internet privacy, (2) stakeholders' views on potential actions to enhance federal oversight of consumers' Internet privacy, and (3) breaches of personally identifiable information. This statement is primarily based on our January 2019 report on Internet privacy.[1] This work included evaluating FTC's Internet privacy enforcement actions and authorities and interviewing various stakeholders, including representatives from industry, consumer advocacy groups, and academia, as well as FTC staff and former FTC and Federal Communications Commission (FCC) commissioners. We also interviewed officials from other federal oversight agencies—such as the Consumer Financial Protection Bureau (CFPB), Food and Drug Administration (FDA), and the Equal Employment Opportunity Commission (EEOC)—about the strengths and limitations of their regulatory and enforcement authorities and approaches. A complete description of our scope and methodology can be found in our January 2019 report. This statement also includes some additional information on data breaches from our August 2018 report on Equifax.[2]

[1]GAO, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility,* GAO-19-52 (Washington, D.C.: Jan. 15, 2019).

[2]GAO, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*, GAO-18-559 (Washington, D.C.: Aug. 30, 2018).

We conducted the performance audit on which this statement is primarily based from October 2017 through January 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In April 2018, Facebook disclosed that a Cambridge University researcher may have improperly shared the data of up to 87 million of Facebook's users with a political consulting firm. This followed other incidents in recent years involving the misuse of consumers' personal information from the Internet, which about three-quarters of Americans use. These types of incidents have raised public concern because Internet-based services and products, which are essential for everyday social and economic purposes, often collect and use various forms of personal information that could cause users harm if released.

The federal privacy framework for private-sector companies is comprised of a set of tailored laws that govern the use and protection of personal information for specific purposes, in certain situations, or by certain sectors or types of entities. Such laws protect consumers' personal information related to their eligibility for credit, financial transactions, and personal health, among other areas.[3]

We reported in 2013 that no overarching federal privacy law governs the collection and sale of personal information among private-sector companies, including information resellers—companies that collect and resell information on individuals.[4] We found that gaps exist in the federal privacy framework, which does not fully address changes in technology and the marketplace. We recommended that Congress consider legislation to strengthen the consumer privacy framework to reflect the effects of changes in technology and the marketplace. Such legislation has not been enacted.

[3]These laws include the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act.

[4]GAO, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace,* GAO-13-663 (Washington, D.C.: Sept. 25, 2013).

FTC's Role and Authorities for Overseeing Internet Privacy

As we reported in January 2019, FTC is primarily a law enforcement agency with authority to, among other things, address consumer concerns about Internet privacy, both for Internet service providers and content providers. It does so using its general authority under section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[5]

Even though the FTC Act does not speak in explicit terms about protecting consumer privacy, the Act authorizes such protection to the extent it involves practices FTC defines as unfair or deceptive. According to FTC, an act or practice is "unfair" if it causes, or is likely to cause, substantial injury not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition as a result of the practice. FTC has used this "unfairness" authority to address situations where a company has allegedly failed to properly protect consumers' data, for example. According to FTC, a representation or omission is "deceptive" if it is material and is likely to mislead consumers acting reasonably under the circumstances. FTC has applied this "deceptiveness" authority to address deceptions related to violations of written privacy policies and representations concerning data security, for example.

FTC staff investigate Internet privacy complaints from various sources and also initiate investigations on their own. If FTC staff have reason to believe that an entity is engaging in an unfair or deceptive practice, they may forward an enforcement recommendation to the commission. The commission then determines whether to pursue an enforcement action.[6] With certain exceptions, FTC generally cannot directly impose civil monetary penalties for Internet privacy cases. Instead, FTC typically addresses Internet privacy cases by entering into settlement agreements requiring companies to take actions such as implementing reasonable privacy and security programs. If a company then violates its settlement agreement with FTC, the agency can request civil monetary penalties in court for the violations. In addition, FTC can seek to impose civil monetary penalties directly for violations of certain statutes and their

[5]15 U.S.C. § 45(a)(1).

[6]FTC staff operate separately from the FTC commission itself, which is the set of five commissioners, including the chair, who ultimately have responsibility for deciding upon courses of action, including enforcement actions.

implementing regulations, such as the statute pertaining to the Internet privacy of children and its corresponding regulations.

FTC has not promulgated rules under section 5 specific to Internet privacy. According to FTC staff, the process the agency must use to issue such rules—known as the Magnuson-Moss procedures—includes steps that add time and complexity to the rulemaking process. FTC has not promulgated any regulations using the Magnuson-Moss procedures since 1980. Although FTC has not implemented its section 5 authority by issuing regulations regarding internet privacy, it has issued regulations when directed and authorized by Congress to implement other statutory authorities using a different set of rulemaking procedures. These procedures, spelled out in section 553 of the Administrative Procedures Act (APA),[7] are those that most federal agencies typically use to develop and issue regulations.

APA section 553 establishes procedures and requirements for what is known as "informal" rulemaking, also known as notice-and-comment rulemaking. Among other things, section 553 generally requires agencies to publish a notice of proposed rulemaking in the *Federal Register*. After giving interested persons an opportunity to comment on the proposal by providing "data, views, or arguments," the statute then requires the agency to publish the final rule in the *Federal Register.*

In contrast, the rulemaking procedures that FTC generally must follow to issue rules under the FTC Act are the Magnuson-Moss procedures noted above. These are required by the Magnuson-Moss Warranty Act amendments to the FTC Act and impose additional rulemaking steps beyond APA section 553. These steps include providing the public and certain congressional committees with an advance notice of proposed rulemaking (in addition to the notice of proposed rulemaking). FTC's rulemaking under Magnuson-Moss also calls for, among other things, oral hearings, if requested, presided over by an independent hearing officer, and preparation of a staff report after the conclusion of public hearings, giving the public the opportunity to comment on the report.

FTC has promulgated regulations using the APA section 553 notice-and-comment rulemaking procedures when authorized or directed by specific statutes. For example, the 1998 Children's Online Privacy Protection Act

[7]5 U.S.C. § 553.

(COPPA) required FTC to issue regulations concerning children's online privacy; promulgate these regulations using the APA section 553 process; and, in determining how to treat a violation of the rules, to treat it as an unfair or deceptive act or practice in most cases. COPPA governs the online collection of personal information from children under the age of 13 by operators of websites or online services, including mobile applications. COPPA contained a number of specific requirements that FTC was directed to implement by regulation, such as requiring websites to post a complete privacy policy, to notify parents directly about their information collection practices, and to obtain verifiable parental consent before collecting personal information from their children or sharing it with others.

Laws and regulations may be enforced in various ways, for example, by seeking civil monetary penalties for non-compliance. As mentioned, FTC has authority to seek civil monetary penalties when a company violates a settlement agreement or certain statutes or regulations. For example, in March 2018, FTC announced that it is investigating whether Facebook's current privacy practices violate a settlement agreement that the company entered into with FTC. In the case that resulted in the 2012 settlement, FTC had charged Facebook with deceiving consumers by telling them they could keep their information private, but then allowing it to be shared and made public. FTC also has authority to seek civil monetary penalties for violations of the COPPA statute as well as FTC's COPPA regulations.

In our January 2019 Internet privacy report, we found that during the last decade, FTC filed 101 Internet privacy enforcement actions to address practices that the agency alleged were unfair, deceptive, a violation of COPPA, a violation of a settlement agreement, or a combination of those reasons. Most of these actions pertained to first-time violations of the FTC Act for which FTC does not have authority to levy civil monetary penalties. In nearly all 101 cases, companies settled with FTC, which required the companies to make changes in their policies or practices as part of the settlement.

Stakeholders and FTC Identified Potential Actions to Enhance Federal Oversight of Consumers' Internet Privacy

Various stakeholders we interviewed for our January 2019 Internet privacy report said that opportunities exist for enhancing Internet privacy oversight. Most industry stakeholders said they favored FTC's current approach—direct enforcement of its unfair and deceptive practices statutory authority, rather than promulgating and enforcing regulations implementing that authority. These stakeholders said that the current approach allows for flexibility; that regulations could hinder innovation, create loopholes, and become obsolete; and that rulemakings can be lengthy. Other stakeholders, including consumer advocates and most former FTC and FCC commissioners we interviewed, favored having FTC issue and enforce regulations. Stakeholders said that regulations can provide clarity, flexibility, and act as a deterrent, and may also promote fairness by giving companies notice of what actions are prohibited.

Those stakeholders who believe that FTC's current authority and enforcement approach is unduly limited identified three main actions that could better protect Internet privacy: (1) enactment of an overarching federal privacy statute to establish general requirements governing Internet privacy practices of all sectors, (2) APA section 553 notice-and-comment rulemaking authority, and (3) civil penalty authority for any violation of a statutory or regulatory requirement, rather than allowing penalties only for violations of settlement agreements or consent decrees that themselves seek redress for a previous statutory or regulatory violation.

Privacy Statute

Stakeholders from a variety of perspectives—including academia, industry, consumer advocacy groups, and former FTC and FCC commissioners—told us that a statute could enhance Internet privacy oversight by, for example, clearly articulating to consumers, industry, and privacy enforcers what behaviors are prohibited. Some stakeholders suggested that such a framework could either designate an existing agency (such as FTC) as responsible for privacy oversight or create a new agency. For example, in Canada, the Office of the Privacy Commissioner, an independent body that reports directly to the Parliament, was established to protect and promote individuals' privacy rights.

Some stakeholders also stated that the absence of a comprehensive Internet privacy statute affects FTC's enforcement. For example, a former federal enforcement official from another oversight agency said that FTC is limited in how it can use its authority to take action against companies' unfair and deceptive trade practices for problematic Internet privacy practices. Similarly, another former federal enforcement official from

another agency said that FTC is limited in how and against whom it can use its unfair and deceptive practices authority noting, for example, that it cannot pursue Internet privacy enforcement against exempted industries.[8]

In addition, some stakeholders said FTC's section 5 unfair and deceptive practices authority may not enable it to fully protect consumers' Internet privacy because it can be difficult for FTC to establish that Internet privacy practices are legally unfair. Because of this difficulty, some stakeholders said that FTC relies more heavily on its authority to take enforcement action against deceptive trade practices compared with the agency's unfair trade practices authority. This is consistent with the results of our analysis of FTC cases, which showed that in a majority of the actions FTC settled, FTC alleged that companies engaged in practices that were deceptive. Furthermore, a recently decided federal appeals court case illustrates potential limits on FTC's enforcement remedies. The court found that FTC could not direct the company, which was accused of unfair practices, to create and implement comprehensive data security measures for the personal information the company stored on its computer networks as a remedy for the practices alleged. Instead, the court ruled that FTC's authority was limited to prohibiting specific illegal practices.[9]

APA Notice-and-Comment Rulemaking

Various stakeholders said that there are advantages to overseeing Internet privacy with a statute that provides APA section 553 notice-and-comment rulemaking authority. Officials from other consumer and worker protection agencies we interviewed described their enforcement authorities and approaches. For example, officials from CFPB and FDA, both of which use APA section 553 notice-and-comment rulemaking, said that their rulemaking authority assists in their oversight approaches and supports their enforcement actions. EEOC officials said that regulations are used to guide investigations that establish whether enforcement action is appropriate.

[8]The FTC Act prohibits FTC from taking action against companies such as telecommunications carriers, airlines and railroads under certain circumstances. FTC also does not have jurisdiction over banks, credit unions, or savings and loans institutions.

[9]In this case, FTC filed a complaint against LabMD, a medical laboratory, under section 5 of the FTC Act for allegedly committing an unfair act or practice by failing to provide reasonable and appropriate security for personal information on its computer networks. On appeal, the Eleventh Circuit ruled that FTC's cease and desist order exceeded its authority because it did not prohibit a specific act or practice but instead, mandated a complete overhaul of the company's data-security program. *LabMD, Inc. v. FTC*, 891 F.3d 1286 (11th Cir. 2018).

Ability to Levy Civil Penalties for Initial Violations

Some stakeholders suggested that FTC's ability to levy civil penalties could also be enhanced. As noted, FTC can levy civil penalties against companies for violating certain regulations, such as COPPA regulations, or for violating the terms of a settlement agreement already in place. According to most former FTC commissioners and some other stakeholders we interviewed, FTC should be able to levy fines for initial violations of section 5 of the FTC Act. An academic told us that the power of an agency to levy a fine is a tangible way to hold industries accountable.

Breaches Involving Personally Identifiable Information Highlight the Importance of Security and Privacy

Recent data breaches at federal agencies, retailers, hospitals, insurance companies, consumer reporting agencies, and other large organizations highlight the importance of ensuring the security and privacy of personally identifiable information collected and maintained by those entities. Such breaches have resulted in the potential compromise of millions of Americans' personally identifiable information, which could lead to identity theft and other serious consequences. For example, the breach of an Equifax online dispute portal from May to July 2017 resulted in the compromise of records containing the personally identifiable information of at least 145.5 million consumers in the United States and nearly 1 million consumers outside the United States. We reported in August 2018 that Equifax's investigation of the breach identified four major factors—identification, detection, segmenting of access to databases, and data governance—that allowed the attacker to gain access to its network and extract information from databases containing personally identifiable information.[10] In September 2017, FTC and CFPB, which both have regulatory and enforcement authority over consumer reporting agencies such as Equifax, initiated an investigation into the breach and Equifax's response. Their investigation is ongoing.

According to a 2017 National Telecommunications and Information Administration (NTIA) survey conducted by the U.S. Census Bureau, 24 percent of American households surveyed avoided making financial transactions on the Internet due to privacy or security concerns.[11] NTIA's survey results show that privacy concerns may lead to lower levels of economic productivity if people decline to make financial transactions on

[10]GAO-18-559.

[11]NTIA, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds* (Washington, D.C.: Aug. 20, 2018) *available at* https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds (last visited Mar. 5, 2019).

the Internet. Consumers who were surveyed indicated that their specific concerns were identity theft, credit card or banking fraud, data collection by online services, loss of control over personal information, data collection by government, and threats to personal safety.

Recent data breaches and developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider what additional actions are needed to protect consumer privacy, including comprehensive Internet privacy legislation. Although FTC has been addressing Internet privacy through its unfair and deceptive practices authority and FTC and other agencies have been addressing this issue using statutes that target specific industries or consumer segments, the lack of a comprehensive federal privacy statute leaves consumers' privacy at risk. Comprehensive legislation addressing Internet privacy that establishes specific standards and includes APA notice-and-comment rulemaking and first-time violation civil penalty authorities could enhance the federal government's ability to protect consumer privacy, provide more certainty in the marketplace as companies innovate and develop new products using consumer data, and provide better assurance to consumers that their privacy will be protected. In our January 2019 report, we recommended that Congress consider developing comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving Internet environment. Issues that should be considered include:

- which agency or agencies should oversee Internet privacy;
- what authorities an agency or agencies should have to oversee Internet privacy, including notice-and-comment rulemaking authority and first-time violation civil penalty authority; and
- how to balance consumers' need for Internet privacy with industry's ability to provide services and innovate.

Chairman Portman, Ranking Member Carper, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For further information regarding this testimony, please contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov or Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

Individuals who made key contributions to this testimony include Andrew Huddleston, Assistant Director; Kay Kuhlman, Assistant Director; Bob Homan, Analyst-in-Charge; Melissa Bodeau; John de Ferrari; Camilo Flores; Nick Marinos, and Sean Standley.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548