United States Government Accountability Office

Testimony

Before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, June 11, 2019

CONSUMER PRIVACY

Changes to Legal Framework Needed to Address Gaps

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

June 2019

CONSUMER PRIVACY

Changes to Legal Framework Needed to Address Gaps

GAO Highlights

Highlights of GAO-19-621T, a testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate

Why GAO Did This Study

Information resellers—companies that collect and resell information on individuals—have dramatically increased the collection and sharing of personal data in recent years, raising privacy concerns. Increasing use of social media, mobile applications, and other technologies have intensified these concerns.

This statement is primarily based on findings from GAO's 2013 report on information resellers (GAO-13-663). It also discusses a 2015 report on facial recognition technology (GAO-15-621), a 2018 report on financial technology (GAO-18-254), and two 2019 reports on internet privacy and consumer data protection (GAO-19-52 and GAO-19-196, respectively). GAO discusses (1) existing federal laws related to the privacy of consumer information held by information resellers and (2) any gaps in this legal framework. For the prior work, GAO analyzed relevant laws, regulations, and enforcement actions and interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and resellers.

What GAO Recommends

In 2013, GAO recommended that Congress consider strengthening the consumer privacy framework to reflect the effects of changing technologies and markets. In 2019, GAO recommended that Congress consider comprehensive internet privacy legislation. Legislation on these issues has not been enacted to date.

View GAO-19-621T. For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov.

What GAO Found

In recent years, GAO issued reports that relate to information resellers and consumer privacy issues. Two central findings from a 2013 GAO report remain current:

- **No overarching federal privacy law governs the collection and sale of personal information among private-sector companies**, including information resellers (data brokers). Instead, a variety of laws are tailored to specific purposes, situations, or entities. For example, the Fair Credit Reporting Act limits use and distribution of personal information collected or used to help determine eligibility for such things as credit or employment. Other laws apply to health care providers, financial institutions, or to online collection of information about children.

- **Gaps exist in the federal privacy framework**. With regard to data that private-sector entities use for marketing, no federal statute provides consumers the right to learn what information is held about them and who holds it. In many cases, consumers also do not have the legal right to control the collection or sharing with third parties of sensitive personal information (such as their shopping habits and health interests) for marketing purposes. In 2013 and in 2015, GAO also reported that the statutory framework for consumer privacy did not fully address new technologies—such as online tracking and facial recognition—and the vastly increased marketplace for personal information, including the proliferation of information sharing among third parties.

  In two 2019 reports, GAO found additional gaps in the federal privacy framework and potential limitations in regulatory authority under current privacy law. Internet content providers and internet service providers collect, use, and share information from customers to enable their services, support advertising, and for other purposes. Although the Federal Trade Commission (FTC) generally has addressed internet privacy through its unfair and deceptive practices authority, and other agencies have used industry-specific statutes, there is no comprehensive federal privacy statute with specific internet privacy standards for the private sector. GAO also reported that the Gramm-Leach-Bliley Act, a key law governing the security of consumer information, does not provide FTC with civil penalty authority for violations of the privacy and data security provisions of the act. New and more advanced technologies and changes in the marketplace for consumer information have vastly increased the amount and nature of personal information collected and the number of parties using or sharing it. Such changes warrant reconsideration of how well the current privacy framework protects personal information.

Chairman Crapo, Ranking Member Brown, and Members of the Committee:

I am pleased to be here today to discuss our prior work on privacy, personal information, and information resellers. Information resellers (also known as data brokers) are companies that collect and resell information on individuals. Privacy concerns about resellers stem, in part, from consumers not always knowing what personal information is collected and how it is used. Moreover, growing use of the internet, social media, and mobile applications has intensified privacy concerns because these media make it much easier to gather personal information, track online behavior, and monitor individuals' locations and activities.

My remarks today are primarily based on our September 2013 report on privacy issues related to the consumer data that information resellers collect, use, and sell, and on our 2015 and 2019 High Risk Reports.[1] In 2013, we found that the framework of federal laws relating to the privacy of consumer information had gaps. We recommended that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace. In our 2015 High Risk Report, we expanded an area of concern—cybersecurity—to include protecting the privacy of personally identifiable information.[2] We also conducted more recent work in the consumer privacy area on facial recognition technology, financial technology, internet privacy, and consumer data protection.[3] In our 2019 High Risk Report, we reiterated our recommendation that Congress consider what additional actions are needed to protect consumer privacy.[4] My statement will focus on the (1)

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

[2]Every 2 years, we report on federal programs and operations that are vulnerable to waste, fraud, abuse, and mismanagement, or that need broad reform—our High Risk List. See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[3]GAO, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law*, GAO-15-621 (July 30, 2015); *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight*, GAO-18-254 (Mar. 22, 2018); *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility*, GAO-19-52 (Jan. 15, 2019); and *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies*, GAO-19-196 (Washington, D.C.: Feb. 21, 2019).

[4]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

existing federal laws and regulations related to the privacy of consumer information held by information resellers and (2) any gaps that may exist in this legal framework.

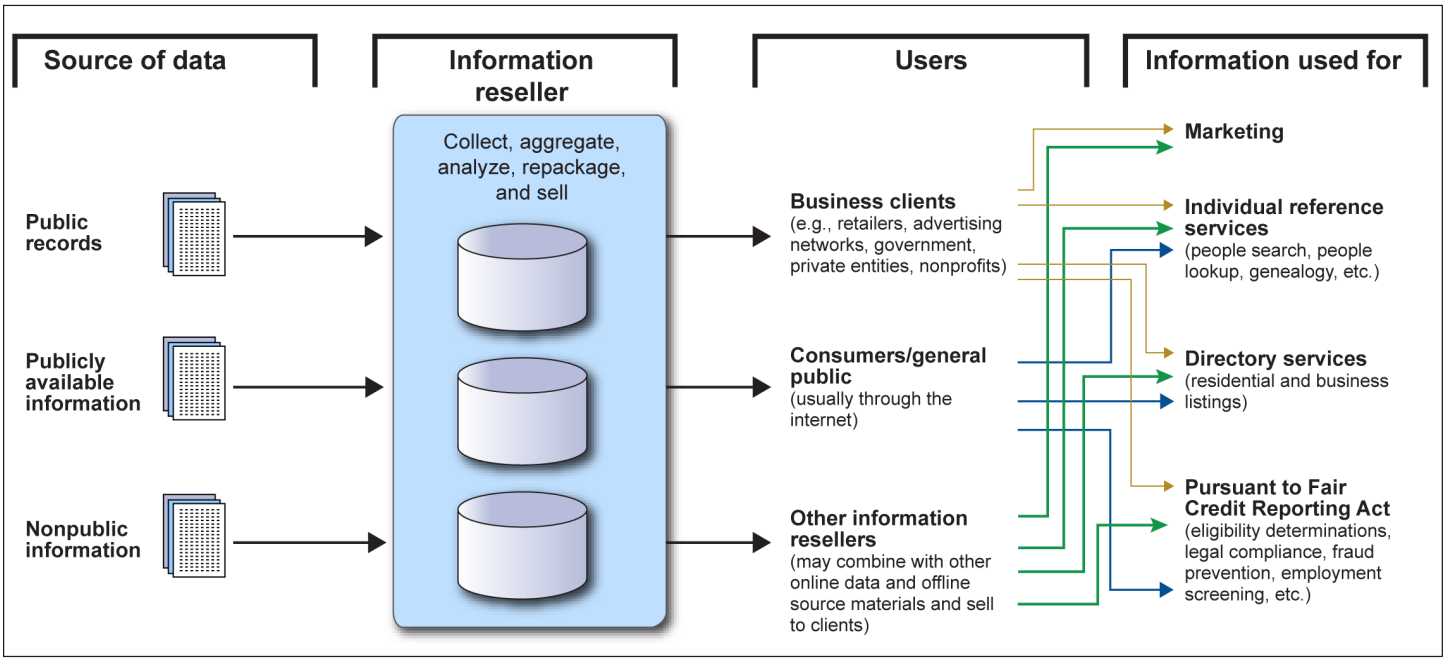
For our September 2013 report (GAO-13-663), we reviewed and analyzed relevant laws, regulations, and enforcement actions. We interviewed representatives of federal agencies, trade associations, consumer and privacy groups, and resellers to obtain their views on data privacy laws related to resellers. The work for our 2015 report on facial recognition technology (GAO-15-621), 2018 report on financial technology (GAO-18-254), and January and February 2019 reports on internet privacy and consumer data protection (GAO-19-52 and GAO-19-196) included analyzing laws and regulations and interviewing representatives of federal agencies, regulators in other countries, market participants, consumer advocacy groups, and academia. For this statement, we verified that findings of our previous reports about gaps in the statutory framework for consumer information privacy remain relevant. More details about our scope and methodology can be found in our published reports.

We conducted the performance audit on which the majority of this statement is based from August 2012 through September 2013, 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

Resellers maintain large, sophisticated databases with consumer information that can include credit histories, insurance claims, criminal records, employment histories, incomes, ethnicities, purchase histories, and interests. As shown in figure 1, resellers largely obtain their information from public records, publicly available information (such as directories and newspapers), and nonpublic information (such as from retail loyalty cards, warranty registrations, contests, and web browsing).

Figure 1: Typical Flow of Consumer Data through Resellers to Third-Party Users



Source: GAO. | GAO-19-621T

Consumer information can be derived from mobile networks, devices (including smartphones and tablets), operating systems, and applications. Resellers also may obtain personal information from the profile or public information areas of websites, including social media sites, or from information on blogs or discussion forums. Depending on the context, information from these sources may be publicly available or nonpublic.

In 1973, a U.S. government advisory committee first proposed the Fair Information Practice Principles for protecting the privacy and security of personal information. While these principles are not legal requirements, they provide a framework for balancing privacy with other interests. In 2013, the Organisation for Economic Co-operation and Development (OECD) developed a revised version of the principles (see table 1).[5]

[5]Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Paris, France: Sept. 23, 1980). OECD's 30 member countries include the United States. OECD has been considering whether to revise or update its privacy guidelines to account for changes in the role of personal data in the economy and society.

Table 1: Fair Information Practice Principles

Principle	Description
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for purposes other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organisation for Economic Co-operation and Development. | GAO-19-621T

The Fair Information Practice Principles served as the basis for the Privacy Act of 1974—which governs the collection, maintenance, use, and dissemination of personal information by federal agencies.[6] The principles also were the basis for many Federal Trade Commission (FTC) and Department of Commerce privacy recommendations and for a framework for consumer data privacy the White House issued in 2012.[7]

[6]*See* Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a). The act generally prohibits (with a number of exceptions) the disclosure by federal entities of records about an individual without the individual's written consent and provides U.S. persons with a means to seek access to and amend their records.

[7]The framework included a consumer privacy bill of rights and encouraged Congress to provide FTC with enforcement authorities for the bill of rights. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, D.C.: Feb. 23, 2012).

Several Laws Apply in Specific Circumstances to Consumer Data That Resellers Hold

As we reported in 2013 and as continues to be the case, no overarching federal privacy law governs the collection, use, and sale of personal information among private-sector companies, including information resellers. There are also no federal laws designed specifically to address all the products sold and information maintained by information resellers. Federal laws addressing privacy issues in the private sector are generally narrowly tailored to specific purposes, situations, types of information, or sectors or entities—such as data related to financial transactions, personal health, and eligibility for credit. These laws include provisions that limit the disclosure of certain types of information to a third party without an individual's consent, or prohibit certain types of data collection. The primary laws include the following:

Fair Credit Reporting Act (FCRA).[8] FCRA protects the security and confidentiality of personal information collected or used to help make decisions about individuals' eligibility for credit, insurance, or employment.[9] It applies to consumer reporting agencies that provide consumer reports.[10] Accordingly, FCRA applies to the three nationwide consumer reporting agencies (commonly called credit bureaus) and to any other information resellers that resell consumer reports for use by others. FCRA limits resellers' use and distribution of personal data—for example, by allowing consumers to opt out of allowing consumer reporting agencies to share their personal information with third parties for prescreened marketing offers.

Gramm-Leach-Bliley Act (GLBA).[11] GLBA protects nonpublic personal information that individuals provide to financial institutions or that such institutions maintain.[12] GLBA sharing and disclosure restrictions apply to financial institutions or entities that receive nonpublic personal information

[8]Pub. L. No. 91-508, Tit. VI, 84 Stat. 1114, 1128 (1970) (codified as amended at 15 U.S.C. §§ 1681-1681x).

[9]*See* 15 U.S.C. §§ 1681-1681x.

[10]For the definition of "consumer reporting agency," see 15 U.S.C. § 1681a(f). For the definition of "consumer report," see 15 U.S.C. § 1681a(d).

[11]Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

[12]*See* 15 U.S.C. §§ 6801-6802. Subtitle A of Title V of the act contains the privacy provisions relating to the disclosure of nonpublic personal information. 15 U.S.C. §§ 6801-6809.

from such institutions.[13] For example, a third party that receives nonpublic personal information from a financial institution to process consumers' account transactions may not use the information or resell it for marketing purposes.

Health Insurance Portability and Accountability Act of 1996 (HIPAA).[14] HIPAA establishes a set of national standards to protect certain health information. The HIPAA privacy rule governs the use and disclosure of an individual's health information for purposes including marketing.[15] With some exceptions, the rule requires an individual's written authorization before a covered entity—a health care provider that transmits health information electronically in connection with covered transactions, health care clearinghouse, or health plan—may use or disclose the information for marketing.[16] The rule does not directly restrict the use, disclosure, or resale of protected health information by resellers or others not considered covered entities under the rule.

Children's Online Privacy Protection Act of 1998 (COPPA).[17] COPPA and its implementing regulations apply to the collection of information—such as name, email, or location—that would allow someone to identify or contact a child under 13.[18] Covered website and online service operators must obtain verifiable parental consent before collecting such information. COPPA may not directly affect information resellers, but the covered entities are potential sources of information for resellers.

[13]15 U.S.C. § 6802. A "financial institution" is any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)). 15 U.S.C. § 6809(3)(a).

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

[15]45 C.F.R. Parts 160, 164.

[16]For the definition of "marketing," including exceptions, *see* 45 C.F.R. § 164.501.

[17]Pub. L. No. 105-277, Div. C, Tit. XIII, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501-6506).

[18]FTC issued regulations implementing COPPA at 16 C.F.R. Part 312.

Electronic Communications Privacy Act of 1986 (ECPA).[19] ECPA prohibits the interception and disclosure of electronic communications by third parties unless an exception applies (such as one party to the communication consenting to disclosure). For example, the act would prevent an internet service provider from selling the content of its customers' emails to a reseller for marketing purposes, unless the customers had consented to disclosure. However, ECPA provides more limited protection for information considered to be "non-content," such as a customer's name and address.

Federal Trade Commission Act (FTC Act), Section 5.[20] The FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. Although the act does not explicitly grant FTC the specific authority to protect privacy, FTC has interpreted it to apply to deceptions or violations of written privacy policies. For example, if a retailer's written privacy policy stated customers' personal information would not be shared with resellers and the retailer later sold information to such parties, FTC could bring an enforcement action against the retailer for unfair and deceptive practices.

Some states also have enacted laws designed to regulate resellers' sharing of personal information about consumers. For example, in 2018, Vermont passed a law that contains, among other requirements, consumer protection provisions related to data brokers.[21] Among other things, the law requires data brokers to register annually and prohibits the acquisition and use of brokered personal information through certain means and for certain uses.

[19]Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

[20]15 U.S.C. § 45. Section 5 of the FTC Act, as originally enacted, only related to "unfair methods of competition." The Wheeler-Lea Act, passed in 1938, expanded the Commission's jurisdiction to include "unfair or deceptive acts or practices." Wheeler-Lea Amendments of 1938, Pub. L. No. 75-447, 52 Stat. 111 (1938).

[21] VT. STAT. ANN. tit. 9, §§ 2430, 2433, 2446 and 2447. Data broker means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. 9 V.S.A. § 2430(4).

Gaps Exist in the Consumer Privacy Framework

The scope of consumer privacy protections provided under federal law has remained narrow in relation to (1) individuals' ability to access, control, and correct their personal data; (2) collection methods and sources and types of consumer information collected; (3) new technologies; and (4) some regulatory authorities. The examples in the following sections are drawn from our earlier reports and remain pertinent today.

Federal Law Provides Individuals Limited Ability to Access, Control, and Correct Their Personal Data

In our 2013 report, we found that no federal statute that we examined generally requires resellers to allow individuals to review personal information (intended for marketing purposes), control its use, or correct it. The Fair Information Practice Principles state that individuals should be able to know about and consent to the collection of their information and have the right to access the information, request correction, and challenge the denial of those rights.

We also reported in 2013 that no federal statute provides consumers the right to learn what information is held about them and who holds it for marketing or look-up purposes. FCRA provides individuals with certain access rights, but only when information is used for credit eligibility purposes. And GLBA's provisions allowing consumers to opt out of having their personal information shared with third parties apply only in specific circumstances. Otherwise, under federal law, individuals generally cannot require that their personal information not be collected, used, and shared. Also, no federal law we examined provides correction rights (the ability to have resellers and others correct or delete inaccurate, incomplete, or unverifiable information) for marketing or look-up purposes.

Laws Largely Do Not Address Data Collection Methods, Sources, and Types

Our 2013 report also found that federal privacy laws are limited in addressing the methods by which, or the sources from which, resellers collect and aggregate personal information, or the types of information collected for marketing or look-up purposes. The Fair Information Practice Principles state that personal information should be relevant, limited to the purpose for which it was collected, and collected with the individual's knowledge or consent.

Federal laws generally do not govern the methods resellers may use to collect personal information. For instance, resellers, advertisers, and others use software to search the web for information about individuals and extract and download bulk information from websites with consumer

information. Resellers or retailers also may collect information indirectly (by combining information from transactions).

Current federal law generally allows resellers to collect personal information from sources such as warranty registration cards and surveys and from online sources such as discussion boards, social media sites, blogs, and web browsing histories and searches. Current federal law generally does not require disclosure to consumers when their information is collected from these sources.

The federal laws that address the types of consumer information that can be collected and shared are not comprehensive. Under most circumstances, information that many people may consider very personal or sensitive can be collected, shared, and used for marketing. This can include information about physical and mental health, income and assets, political affiliations, and sexual habits and orientation. For health information, HIPAA rule provisions generally apply only to covered entities, such as health care providers.

Privacy Framework Largely Has Not Kept Pace with Changes in Technology

The current privacy framework does not fully address new technologies such as facial recognition technology, privacy issues raised by online tracking and mobile devices, and activities by financial technology firms. The original enactment of several federal privacy laws predates these trends and technologies. But in some instances existing laws have been interpreted to apply to new technologies. For example, FTC has taken enforcement actions under COPPA and revised the statute's implementing regulations to account for smartphones and mobile applications.

Facial Recognition Technology

One example of how privacy law has not kept pace with changes in technology is the use of facial recognition technology, which involves the collection of facial images and may be employed in a wide range of commercial applications. In our 2015 report we concluded that the future trajectory of this technology raised questions about consumer privacy.[22] We found that federal law does not expressly address the circumstances under which commercial entities can use facial recognition technology to identify or track individuals, or when consumer knowledge or consent should be required for the technology's use. Furthermore, in most

[22]GAO-15-621.

contexts federal law does not address how personal data derived from the technology may be used or shared. The privacy issues stakeholders raised about facial recognition technology and other biometric technologies in use at the time of our 2015 report served as yet another example of the need to adapt federal privacy law to reflect new technologies. As such, we reiterated our 2013 recommendation that Congress strengthen the current consumer privacy framework to reflect the effects of changes in technology and the marketplace.

Activities by Financial Technology Firms

The rise of financial services provided by nonfinancial firms—often referred to as fintech—is another example of how new technology may create privacy concerns. For example, fintech lenders offer a variety of loans such as consumer and small business loans and operate almost exclusively online. In our 2018 report, we noted that while these lenders may still assess borrowers' creditworthiness with credit scores, they also may analyze large amounts of additional or alternative sources of data to determine creditworthiness.[23] We also found that some fintech firms may collect more consumer data than traditional lenders. For example, fintech lenders may have sensitive information such as consumers' educational background or utility payment information, and according to certain stakeholders, these data may contain errors that cannot be disputed by consumers under FCRA.

Furthermore, some data aggregators may hold consumer data without disclosing what rights consumers have to delete the data or prevent the data from being shared with other parties. A leak of these or other data held by fintech firms may expose characteristics that people view as sensitive. GLBA generally requires fintech firms and traditional financial institutions to safeguard nonpublic personal information about customers.[24] Our 2018 report discussed that some fintech firms use new technologies or mobile device features to mitigate data privacy risks and that some regulators have issued guidance to consumers publicizing practices that help maintain privacy when using online products and services, including those provided by fintech firms. Regulators also have issued GLBA guidance to businesses, including fintech firms, recommending that they adopt policies and procedures to prevent, detect, and address privacy threats.

[23]GAO-18-254.

[24]GLBA restricts, with some exceptions, the disclosure of nonpublic information by companies defined as financial institutions. *See* 15 U.S.C. §§ 6801-6802.

Internet Privacy Issues

Online tracking. In our 2013 report, we found that no federal privacy law explicitly addresses the full range of practices to track or collect data from consumers' online activity. Cookies allow website operators to recall information such as user name and address, credit card number, and purchases in a shopping cart. Resellers can match information in cookies and their databases to augment consumer profiles. Third parties also can synchronize their cookie files with resellers' files. Advertisers can use third-party cookies—placed on a computer by a domain other than the site being visited—to track visits to the websites on which they advertise. While current federal law does not, with some exceptions, explicitly address web tracking, FTC has taken enforcement actions related to web tracking under its authority to enforce the prohibition on unfair or deceptive acts. For example, in 2011, FTC settled charges with Google for $22.5 million after alleging that Google violated an earlier privacy settlement with FTC when it misrepresented to users of Apple's Safari web browser that it would not track and serve targeted advertisements to Safari users.[25] Google agreed to disable its advertising tracking cookies.

Mobile devices. In 2013, we also explained that no federal law comprehensively governs applications software for mobile devices. Application developers, mobile carriers, advertisers, and others may collect an individual's information through services provided on a mobile device. However, FTC has taken enforcement action against companies for use of mobile applications that violate COPPA and FCRA.[26] The agency also has taken action under the FTC Act.[27] We and others have reported that the capability of mobile devices to provide consumer's location engenders privacy risks, particularly if companies use or share

[25]*United States v. Google Inc.*, No. CV 12-04177-SI, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012).

[26]FTC settled charges that a social networking service deceived consumers when it collected information from children under 13 through its mobile application in violation of COPPA. *See United States v. Path, Inc.*, No. C13-0448 (N.D. Cal. Jan. 31, 2013). FTC also settled charges that a company compiled and sold criminal record reports through its mobile application and operated as a consumer reporting agency, in violation of FCRA. *See In the Matter of Filiquarian Publishing, LLC*, FTC File No. 112 3195 (Apr. 30, 2013).

[27]In addition to the alleged COPPA violation, Path allegedly deceived users by collecting personal information from their mobile address books without their knowledge and consent. *See United States v. Path, Inc.*, No. C13-0448 (N.D. Cal. Jan. 31, 2013).

location data without consumers' knowledge.[28] ECPA might not apply if location data were not deemed content and would not govern entities that are not covered by ECPA. But FTC could pursue enforcement action if a company's collection or use of the information violated COPPA.

More recently, in January of this year, we issued a report on internet privacy that reinforces what we reported in 2013.[29] To varying extents, internet content providers and internet service providers collect, use, and share information from their customers to enable their services, support advertising, and for other purposes. Consumers access such services through mobile phones and tablets, computers, and other internet-connected devices. However, there is no comprehensive federal privacy statute with specific standards. FTC has been addressing internet privacy through its unfair and deceptive practices authority, among other statutes, and other agencies have been addressing this issue using industry-specific statutes. We concluded that recent developments regarding internet privacy suggest that this is an appropriate time for Congress to consider comprehensive internet privacy legislation. To address such privacy concerns, states and other countries have adopted privacy rules. For example, the European Union's General Data Protection Regulation, which came into force in May 2018, is a set of privacy rules that give consumers control over the collection, use, and sharing of their personal information, and California passed its own privacy law in June 2018 that becomes effective in 2020.[30]

Regulatory Authorities under Current Law May Be Limited

In February of this year, we reported that FTC does not have civil penalty authority for initial violations of GLBA's privacy and safeguarding requirements, which, unlike FCRA, includes a provision directing federal regulators and FTC to establish standards for financial institutions to

[28]Risks included disclosure to third parties for unspecified uses, tracking of consumer behavior, and identity theft. See GAO, *Mobile Device Location ID: Additional Federal Actions Could Help Protect Consumer Privacy*, GAO-12-903 (Washington, D.C.: Sept. 11, 2012). A Federal Communications Commission report also noted privacy risks. See Federal Communications Commission, *Location-Based Services: An Overview of Opportunities and Other Considerations* (Washington, D.C.: May 2012).

[29]GAO-19-52.

[30]California's law generally will require companies to report to customers, upon their request, the categories of personal information they collected about the customer, the business or commercial purpose for collecting and selling such personal information, and what categories of third parties received it.

protect against any anticipated threats or hazards to the security of customer records.[31] To obtain monetary redress for these violations, FTC must identify affected consumers and any monetary harm they may have experienced. However, harm resulting from privacy and security violations (such as a data breach) can be difficult to measure and can occur years in the future, making it difficult to trace a particular harm to a specific breach. As a result, FTC lacks a practical enforcement tool for imposing civil money penalties that could help to deter companies from violating data security provisions of GLBA and its implementing regulations. We recommended that Congress consider giving FTC civil penalty authority to enforce GLBA's safeguarding provisions.

Additionally, in our January 2019 report, we found that FTC had not yet issued regulations for internet privacy other than those protecting financial privacy and the internet privacy of children, which were required by law. FTC uses its statutory authority under the FTC Act to protect consumers from unfair and deceptive trade practices. For FTC Act violations, FTC may promulgate regulations but is required to use procedures that differ from traditional notice-and-comment processes and that FTC staff said add time and complexity. In addition, under this authority, FTC can generally only levy civil money penalties after a company has violated an FTC final consent order. In our recommendation that Congress consider developing comprehensive internet privacy legislation, we also suggested that such legislation consider providing rulemaking and civil money penalty authorities to the proper agency or agencies.

In summary, new technologies have vastly changed the amount of personal information private companies collect and how they use it. But our current privacy framework does not fully address these changes. Laws protecting privacy interests are tailored to specific sectors and uses. And, consumers have little control over how their information is collected, used, and shared with third parties for marketing purposes. As a result, current privacy law is not always aligned with the Fair Information Practice Principles, which the Department of Commerce and others have said should serve as the foundation for commercial data privacy. Thus, the privacy framework warrants reconsideration by Congress in relation to consumer interests, new technologies, and other issues.

[31]GAO-19-196.

Chairman Crapo, Ranking Member Brown, and Members of the Committee, this concludes my statement. I would be pleased to respond to any questions you may have.

GAO Contacts

For further information on this statement, please contact Alicia Puente Cackley at 202-512-8678 or cackleya@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this statement. In addition to the contact above, Jason Bromberg (Assistant Director), William R. Chatlos, Rachel DeMarcus, Kay Kuhlman (Assistant Director), Christine McGinty (Analyst in Charge), Barbara Roesmann, and Tyler Spunaugle contributed to this statement. Other staff who made key contributions to the reports cited in the testimony are identified in the source products.