United States Government Accountability Office

Report to the Chairman,
Committee on Energy and Commerce,
House of Representatives

January 2019

# INTERNET PRIVACY

# Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility

Accessible Version

GAO-19-52

GAO Highlights

Highlights of GAO-19-52, a report to the Chairman, Committee on Energy and Commerce, House of Representatives

January 2019

# INTERNET PRIVACY

## Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility

## Why GAO Did This Study

In April 2018, Facebook disclosed that a Cambridge University researcher may have improperly shared the data of up to 87 million of its users with a political consulting firm. This disclosure followed other recent incidents involving the misuse of consumers' personal information from the Internet, which is used by about three-quarters of Americans. GAO was asked to review federal oversight of Internet privacy. This report addresses, among other objectives: (1) how FTC and FCC have overseen consumers' Internet privacy and (2) selected stakeholders' views on the strengths and limitations of how Internet privacy currently is overseen and how, if it all, this approach could be enhanced.

GAO evaluated FTC and FCC Internet privacy enforcement actions and authorities and interviewed representatives from industry, consumer advocacy groups, and academia; FTC and FCC staff; former FTC and FCC commissioners; and officials from other federal oversight agencies. Industry stakeholders were selected to represent different sectors, and academics were selected because of their expertise in privacy, consumer protection, and regulatory issues.

## What GAO Recommends

Congress should 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 what authorities agencies should have in order to oversee Internet privacy, including appropriate rulemaking authority.

View GAO-19-52. For more information, contact Alicia Puente Cackley at (202) 512-8678 or cackleya@gao.gov or Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

## What GAO Found

The United States does not have a comprehensive Internet privacy law governing the collection, use, and sale or other disclosure of consumers' personal information. At the federal level, the Federal Trade Commission (FTC) currently has the lead in overseeing Internet privacy, using its statutory authority under the FTC Act to protect consumers from unfair and deceptive trade practices. However, to date FTC has not issued regulations for Internet privacy other than those protecting financial privacy and the Internet privacy of children, which were required by law. 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 the last decade, FTC has filed 101 enforcement actions regarding Internet privacy; nearly all actions resulted in settlement agreements requiring action by the companies. In most of these cases, FTC did not levy civil penalties because it lacked such authority for those particular violations. The Federal Communications Commission (FCC) has had a limited role in overseeing Internet privacy. From 2015 to 2017, FCC asserted jurisdiction over the privacy practices of Internet service providers. In 2016, FCC promulgated privacy rules for Internet service providers that Congress later repealed. FTC resumed privacy oversight of Internet service providers in June 2018.

Stakeholders GAO interviewed had varied views on the current Internet privacy enforcement approach and how it could be enhanced. Most Internet 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 and that regulations could hinder innovation. Other stakeholders, including consumer advocates and most former FTC and FCC commissioners GAO interviewed, favored having FTC issue and enforce regulations. Some stakeholders said a new data-protection agency was needed to oversee consumer privacy. Stakeholders identified three main areas in which Internet privacy oversight could be enhanced:

- *Statute.* Some stakeholders told GAO that an overarching Internet privacy statute could enhance consumer protection by clearly articulating to consumers, industry, and agencies what behaviors are prohibited.
- *Rulemaking.* Some stakeholders said that regulations can provide clarity, enforcement fairness, and flexibility. Officials from two other consumer protection agencies said their rulemaking authority assists in their oversight efforts and works together with enforcement actions.
- *Civil penalty authority.* Some stakeholders said FTC's Internet privacy enforcement could be more effective with authority to levy civil penalties for first-time violations of the FTC Act.

Comprehensive Internet privacy legislation that establishes specific standards and includes traditional notice-and-comment rulemaking and broader civil penalty authority could enhance the federal government's ability to protect consumer privacy.

# Contents



Tables



Figure



**Abbreviations**

| | |
|---|---|
| APA | Administrative Procedure Act |
| CFPB | Consumer Financial Protection Bureau |
| COPPA | Children's Online Privacy Protection Act |
| CPSC | Consumer Product Safety Commission |
| DOJ | Department of Justice |
| EEOC | Equal Employment Opportunity Commission |

| | |
|---|---|
| FCC | Federal Communications Commission |
| FDA | Food and Drug Administration |
| FTC | Federal Trade Commission |
| FTC Act | Federal Trade Commission Act |
| Magnuson-Moss | Magnuson-Moss Warranty Act amendments to the FTC Act |
| NTIA | National Telecommunications and Information Administration |
| OSH Act | Occupational Safety and Health Act of 1970 |
| OSHA | Occupational Safety and Health Administration |

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 15, 2019

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
House of Representatives

Dear Mr. Chairman:

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 raise public concern because people use the Internet as an essential service for everyday social and economic purposes, and consumer products are increasingly being connected to the Internet.[1] These Internet-based services and products often collect and use various forms of personal information about users, including their location, search terms, contact information, financial information, and many other forms of inherently or potentially sensitive details that could cause users harm if released.

To address such privacy concerns, in May 2018, the European Union implemented the General Data Protection Regulation, a set of Internet privacy rules that give consumers control over the collection, use, and sharing of their personal information. In addition, California passed its own Internet privacy law in June 2018 that becomes effective in 2020. The United States does not have a similar comprehensive data privacy law at the federal level and instead relies in part on an industry-specific (sectoral) privacy approach. This involves 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

[1]For more information on Internet use and connectivity, see GAO, *Broadband: Intended Outcomes and Effectiveness of Efforts to Address Adoption Barriers Are Unclear,* GAO-15-473 (Washington, D.C.: June 2, 2015) and *Internet of Things: Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise,* GAO-17-570 (Washington, D.C.: July 26, 2017).

exceptions. Specifically, FTC addresses consumer concerns about Internet privacy using its broad authority under the FTC Act 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. The common carrier exemption in the FTC Act, however, prohibits FTC from taking action against common carriers, such as providers of telecommunications services.

From 2015 to 2017, the Federal Communications Commission (FCC) classified broadband Internet service as a telecommunications service and asserted statutory and regulatory authority to address privacy concerns related to broadband providers of this service, known as Internet service providers.[2] FCC developed privacy regulations governing these entities in 2016, but Congress repealed the regulations before they took effect. In December 2017, FCC reversed its decision to classify broadband as a telecommunications service, and in June 2018, FTC resumed privacy oversight of Internet service providers.

You asked us to examine issues related to federal oversight of Internet privacy. This report discusses:

- the benefits and concerns associated with the collection of Internet users' personal information for commercial purposes,
- how FTC and FCC have overseen consumers' Internet privacy, and
- selected stakeholders' views on the strengths and limitations of how Internet privacy currently is overseen and how, if it all, this approach could be enhanced.

To determine what is known about the benefits and concerns associated with the collection of Internet users' personal information for commercial purposes, we reviewed public opinion surveys conducted by the Commerce Department's National Telecommunications and Information Administration (NTIA) in 2017 and the Pew Research Center in 2015 and

[2]Internet service providers are companies such as Verizon that provide consumers and small businesses access to the Internet. This service could be a fixed service at home offered by, for example, cable or fiber or a mobile service accessible at or away from home with a mobile device.

2018,[3] prior GAO reports, and other related literature. For this and the other objectives, we interviewed FTC and FCC staff; NTIA officials; stakeholders from 4 consumer advocacy groups and 4 industry groups; 6 Internet service providers; 6 Internet content providers;[4] and 11 academics about Internet privacy. To obtain a variety of perspectives, we selected 6 Internet service providers that represented different industry sectors (i.e., cable, satellite, and telephone-based Internet service) and 6 Internet content providers that provide a variety of information and social media services. Academic stakeholders were selected because of their expertise in privacy, consumer protection, and regulatory issues.[5] We also interviewed a former congressional staff member who has expertise on privacy issues and is now a consultant. Stakeholders were selected to represent a range of views, but our interview results are not generalizable to all stakeholders. Appendix I lists our interviewees.

To address how FTC and FCC have overseen Internet privacy, we analyzed 101 Internet privacy enforcement actions that FTC filed during the last 10 years[6] and an FCC Internet privacy case that was brought during the 2015-2017 period when the agency asserted jurisdiction over

[3]NTIA and the Pew Research Center regularly conduct national surveys on Internet privacy.

[4]Internet content providers are companies such as Facebook that provide various types of Internet-based services, such as social media, streaming media, search, navigation, and online shopping, among many others.

[5]As noted in appendix I, some academics we interviewed were also former FTC officials.

[6]FTC provided us an initial list of Internet privacy enforcement actions, which an FTC staff member said were identified because they involved the unauthorized transmission, collection, or disclosure of personal information. The staff member said that although there are other types of cases, such as those that fall under the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, that could theoretically involve Internet privacy concerns, the cases FTC identified represented substantially all of its Internet privacy cases. Through our search of the FTC website, we identified additional FTC Internet privacy enforcement actions filed by FTC in which the agency alleged a violation of its rule promulgated under the Children's Online Privacy Protection Act and other actions in which FTC alleged that companies made deceptive representations about their participation in international privacy programs. Those additional actions are also included in this report but we did not include actions that fall under the Fair Credit Reporting Act or the Gramm-Leach-Bliley Act. We could not verify that we identified all FTC Internet privacy enforcement actions.

the privacy practices of Internet service providers.[7] We also reviewed FTC and FCC guidance on Internet privacy and enforcement and a memorandum of understanding between FTC and FCC regarding Internet privacy jurisdiction and coordination.

To determine selected stakeholders' views on the strengths and limitations of how Internet privacy currently is overseen and to identify how, if it all, this approach could be enhanced, we reviewed pertinent literature, the legislative history of FTC's statutory rulemaking authorities, and consumer protection statutes and regulations. We also interviewed the stakeholders identified above and eight former FTC and FCC commissioners.[8] We selected to interview former FTC and FCC commissioners who served during the Barack Obama and George W. Bush administrations and are from different political parties. We also interviewed officials from other federal agencies that oversee various industries about the strengths and limitations of their regulatory and enforcement authorities and approaches. The interviews included officials from three consumer protection agencies—the Consumer Financial Protection Bureau (CFPB), the Consumer Product Safety Commission (CPSC), and the Food and Drug Administration (FDA)—and two worker protection agencies—the Occupational Safety and Health Administration (OSHA) and the Equal Employment Opportunity Commission (EEOC). We selected these agencies because they had consumer- or worker-protection responsibilities. In addition, we compared FTC's authorities regarding Internet privacy to characteristics we identified in our prior work that should be reflected in new regulatory systems[9] and to the Fair Information Practice Principles, which are a set of internationally

[7]In this case, FCC fined Verizon Wireless, in part under section 222 of the Communications Act of 1934, codified at 47 U.S.C. § 222. That provision requires every telecommunications carrier to protect the confidentiality of proprietary information of customers. Although the settlement was finalized during the 2015-2017 period, the Verizon Wireless practices occurred prior to the classification of Internet service providers as telecommunications carriers. The investigation, therefore, did not rely upon FCC's assertion of authority over Internet service providers' privacy practices.

[8]Some of the commissioners we interviewed also served as chairs, but we are referring to them collectively as commissioners in this report.

[9]GAO, *Financial Regulation: A Framework for Crafting and Assessing Proposals to Modernize the Outdated U.S. Financial Regulatory System,* GAO-09-216 (Washington, D.C.: Jan. 8, 2009).

developed voluntary principles for protecting the privacy and security of personal information.[10]

This report focuses on Internet data privacy, which is affected by the collection and use of consumers' personal information such as their Internet browsing histories, purchases, locations, and travel routes. Although this report discusses some Internet privacy enforcement actions that also involved data security issues, for the purposes of this review we are distinguishing between Internet data privacy and Internet data security, the latter of which can involve illegal breaches of sensitive information through hacking.

We conducted semi-structured interviews; not all interviewees were asked the same questions. Throughout this report, we use certain qualifiers when describing responses from interview participants, such as "some," and "most." We define "some" as three or more but less than half and "most" as a majority of all interviewees or a relevant subset of them.

We conducted this performance audit 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.

[10]The Fair Information Practice Principles are widely accepted non-binding principles for protecting the privacy and security of personal information. In 1973, an early version was proposed by the Advisory Committee on Automated Personal Data Systems, a group convened by the Secretary of Health, Education and Welfare and consisting of outside representatives from private industry, academia, state legislatures and agencies, and elsewhere. The Advisory Committee recommended enactment of a federal "Code of Fair Information Practice" applicable to automated personal data systems. In 1980, the Organisation for Economic Co-Operation and Development (OECD), an organization of 36 member countries, including the United States, created to foster economic development, developed a revised version that was widely adopted.

# Background

## Internet Industry and Consumer Privacy

To varying extents, Internet content providers—also called "edge providers"—and Internet service providers collect, use, and share information from their customers to enable their services, support advertising, and for other purposes. Many companies describe these and other privacy-related practices in privacy policies, to which consumers may be required to consent in order to use the service. Consumers access such services through a variety of devices, including mobile phones and tablets, computers, and other devices connected to the Internet by wired or wireless means.

A nationwide survey that the U.S. Census Bureau conducted for NTIA in 2017 found that 78 percent of Americans ages 3 and older used the Internet. Another nationwide survey that the Pew Research Center conducted in 2018 found that 69 percent of American adults reported that they use some kind of social media platform such as Facebook.

No comprehensive federal privacy law governs the collection, use, and sale or other disclosure of personal information by private-sector companies in the United States. Rather, the federal privacy framework for private-sector companies is comprised partly 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. These laws include the Fair Credit Reporting Act,[11] which protects the security and confidentiality of personal information collected or used to help make decisions about individuals' eligibility for such products as credit or for insurance or employment; the Gramm-Leach-Bliley Act,[12] which protects nonpublic personal information that individuals provide to financial institutions or that such institutions maintain; and the Health Insurance Portability and Accountability Act[13] which establishes a set of

[11]Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. § 1681 *et seq*).

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

[13]Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of Titles 18, 26, 29, and 42 U.S.C.).

national standards for the protection of certain health information. In addition, as detailed in this report, FTC addresses consumer concerns about Internet privacy using its broad authority to protect consumers from unfair and deceptive trade practices.

We have reported on a variety of Internet privacy concerns in recent years that include the collection and use of data such as people's Internet browsing histories, purchases, locations, and travel routes, including:

- **Internet of things:** In 2017, we found that as new and more devices become connected, they increase not only the opportunities for security and privacy breaches, but also the scale and scope of any resulting consequences.[14]
- **Vehicle data privacy:** We found in 2017 that most selected automakers reported limiting their data collection, use, and sharing, but their written notices did not clearly identify data sharing and use practices.[15]
- **Information resellers:** In a 2013 report on companies that collect and resell information on individuals, we found that no overarching federal privacy law governs the collection and sale of personal information among private-sector companies, including information resellers.[16] We found that gaps exist in the federal privacy framework, which does not fully address changes in technology and the marketplace. Among the issues we noted were the potential need for changes to privacy controls for web tracking, mobile devices, and other technologies. We recommended that Congress consider strengthening the consumer privacy framework to reflect the effects of changes in technology and the marketplace. Such legislation has not been enacted to date.
- **Mobile device location data:** In 2012, we found that, according to privacy advocates, consumers are generally unaware of how their location data are shared with and used by third parties.[17] We recommended that FTC consider issuing guidance establishing FTC's

[14]GAO-17-570.

[15]GAO, *Vehicle Data Privacy: Industry and Federal Efforts Under Way but NHTSA Needs to Define Its Role,* GAO-17-656 (Washington, D.C.: July 28, 2017).

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

[17]GAO, *Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy,* GAO-12-903 (Washington, D.C.: Sept. 11, 2012).

views regarding mobile companies' appropriate actions to protect location data privacy. FTC implemented that recommendation in 2013.

To guide their privacy practices, many organizations and governments have used the Fair Information Practice Principles. As noted above, these principles—which are not limited to Internet privacy—address the collection and use of personal information, data quality and security, and transparency, among other things, and have served as the basis for many of the privacy recommendations federal agencies have made. The Organisation for Economic Co-Operation and Development developed a version of these principles in 1980 that has been widely adopted and was updated in 2013. In 2000, FTC recommended that Congress enact a consumer Internet privacy statute that would require companies to comply with broad and flexible definitions of the principles,[18] and an FTC commissioner said in a 2014 speech that they are a solid framework and are flexible and effective. While they are principles, not legal requirements, they provide a possible approach for balancing the need for privacy with other interests. Table 1 provides more detailed information about the principles.

**Table 1: Summary of the Organisation for Economic Co-operation and Development's 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, done with the knowledge or consent of the individual. |
| Data quality | Personal information should be relevant to the purpose for which it is collected, and 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 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. |

[18]FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace, a Report to Congress,* May 2000. FTC also recommended in a 2012 privacy framework that Congress consider enacting baseline privacy legislation while industry adopts a privacy framework with practices that FTC stated were consistent with the Fair Information Practice Principles. FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* March 2012.

| Principle | Description |
|---|---|
| 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-19-52

## FTC and FCC Oversight of Internet Privacy

FTC is primarily a law enforcement agency that, among other responsibilities, currently has the lead in overseeing Internet privacy at the federal level. Specifically, it addresses consumer concerns about Internet privacy, both for Internet service providers and content providers, using its general authority under section 5 of the FTC Act. Section 5, as amended in 1938, prohibits "unfair or deceptive acts or practices in or affecting commerce."[19] Although the FTC Act generally empowers FTC to take enforcement action, it prohibits FTC from taking action against common carriers such as telecommunication services, airlines, and railroads under certain circumstances.[20] FTC also does not have jurisdiction over banks, credit unions, or savings and loans institutions.

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. According to FTC, a representation or omission is "deceptive" if it is material and is likely to mislead consumers acting reasonably under the circumstances. For example, the omission of terms in an advertisement would need to be material and likely to mislead

[19]15 U.S.C. § 45(a)(1).

[20]This is referred to as the common carrier exemption. Common carriers are generally entities that provide essential services that can be solicited by the general public.

consumers in order to be deceptive.[21] FTC applies this "deceptive" authority to address deceptions or violations of written privacy policies and representations concerning data security.

FTC's Bureau of Consumer Protection investigates Internet privacy complaints from various sources, including consumers, other agencies, Congress, and industry, and also initiates investigations on its own. If the bureau has reason to believe that an entity is engaging in an unfair or deceptive practice, it may forward an enforcement recommendation to the commission. The commission then determines whether to pursue an enforcement action, which can include the following:

- litigating commission-filed administrative complaints before an FTC administrative law judge;[22]
- filing and litigating complaints in federal district court seeking preliminary and permanent injunctions, monetary redress for consumers or other equitable relief; or
- referring complaints seeking civil penalties for violations of rules authorizing such penalties or for violations of administrative orders to the Department of Justice (DOJ) and assisting DOJ in litigating those cases (if DOJ does not take action, FTC can pursue the action on its own).[23]

FTC's Internet privacy enforcement cases may be settled without the imposition of civil penalties.[24] Instead, FTC typically enters into settlement agreements requiring companies to take actions such as:

- implementing reasonable privacy and security programs;

[21]According to FTC's 1983 Deception Policy Statement, an ad is deceptive if it contains a statement or omits information that is likely to mislead consumers acting reasonably under the circumstances and is "material," that is, important to a consumer's decision to buy or use the product.

[22]Administrative complaints specify the initial charges against an entity.

[23]Civil penalty authority gives an agency the ability to seek a monetary remedy from an entity that has violated a statute or regulation.

[24]FTC lacks authority to impose civil penalties except when the respondent/defendant business has violated an FTC order, a statute (such as the Fair Credit Reporting Act), or a rule (such as FTC's regulations implementing the Children's Online Privacy Protection Act, discussed later) that confers civil penalty authority. The commission lacks authority to seek direct civil penalties for violations of section 5 of the FTC Act.

- being subject to long-term monitoring of compliance with the settlements by outside entities;
- providing monetary redress to consumers;
- forfeiting any money gained from the unfair or deceptive conduct;
- deleting illegally obtained consumer information; and
- providing transparency and choice mechanisms to consumers.

If a company violates an FTC final consent order, the agency can then request civil monetary penalties in court for the violations. In addition, as discussed below, FTC can seek to impose civil monetary penalties directly for violations of certain privacy statutes and regulations such as the statute pertaining to the Internet privacy of children and its implementing regulations. Although FTC can levy civil penalties up to $41,484[25] per violation, per day, against an entity that violates a trade regulation rule under the FTC Act, it has not promulgated trade regulation rules under section 5 specific to privacy.[26]

Although FTC has not implemented its section 5 authority by issuing regulations regarding Internet privacy, it has issued regulations to implement other statutory authorities. Likewise, other federal agencies use regulations to implement the statutes they are charged with administering. The process by which federal agencies typically develop and issue regulations is spelled out in the Administrative Procedure Act (APA). Section 553 of the APA establishes procedures and requirements for what is known as "informal" rulemaking, also known as notice-and-comment rulemaking.[27] 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*. Regulations may be enforced in various ways, for example, by seeking civil penalties for non-compliance. FTC has authority to seek civil

[25]This number is adjusted for inflation.

[26]FTC is authorized to prescribe "trade regulation" rules that define with specificity unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 57a. Those who violate such a rule with knowledge that the act or practice is unfair or deceptive and is prohibited by the rule are liable for civil penalties for each violation. The FTC can obtain the penalties by filing suit in district court. 15 U.S.C. § 45(m)(1)(A).

[27]5 U.S.C. § 553.

penalties, for example, when a company knowingly violates a regulation or, as discussed below, a final consent order.

In contrast to the APA section 553 rulemaking process, the rulemaking process that FTC generally must follow to issue rules under the FTC Act is spelled out in the Magnuson-Moss Warranty Act amendments to the FTC Act (Magnuson-Moss).[28] The Magnuson-Moss amendments—enacted in 1975[29] partly in response to industry opposition to FTC's trade regulations, and amended in 1980[30]—require additional rulemaking steps beyond APA section 553.[31] For example, Magnuson-Moss requires FTC to publish an advance notice of proposed rulemaking in addition to the notice of proposed rulemaking required by the APA, and to offer interested parties the opportunity for an informal hearing involving oral testimony. FTC has not promulgated any regulations using the Magnuson-Moss procedures since 1980; according to FTC staff, the additional steps required under Magnuson-Moss add time and complexity to the rulemaking process.

The Children's Online Privacy Protection Act (COPPA), enacted in 1998, governs the online collection of personal information from children under the age of 13 by operators of websites or online services, including

[28]15 U.S.C. § 57a.

[29]Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, § 202(d), 88 Stat. 2183, 2198 (1975).

[30]Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, § 11, 94 Stat. 374, 398 (1980).

[31]From 1970-1978, Congress enacted various "hybrid" rulemaking statutes that combine elements of formal and informal rulemaking, such as the Magnuson-Moss Warranty Act. As explained above, section 553 of the APA establishes requirements for "informal," notice-and-comment rulemaking. APA sections 556 and 557 establish requirements for "formal" rulemaking, which involve more trial-type procedures. One administrative law expert attributes enactment of these hybrid rulemaking statutes to the growing complexity of the issues involved in informal rulemaking, a perceived need to probe the accuracy of public comments, and the strong belief among legislators in the value of communication between regulators and the regulated. *See* Jeffrey S. Lubbers, *A Guide to Federal Agency Rulemaking* 282 (5th ed. 2014). Furthermore, the legislative history of the FTC Improvements Act of 1980, which amended Magnuson-Moss, reflects that at least some legislators believed additional rulemaking procedures would "be very useful in helping Congress look over the shoulder of the FTC to guarantee that the rules the agency issues are really in keeping with the intent of Congress." 117 Cong. Rec. 29,746 (1979) (statement of Rep. Broyhill).

mobile applications.[32] COPPA required FTC to issue and enforce regulations concerning children's online privacy and directed FTC to promulgate these regulations using the APA section 553 notice-and-comment rulemaking process.[33] 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. The commission's original COPPA regulations became effective on April 21, 2000,[34] and amended COPPA regulations[35] took effect on July 1, 2013.[36] According to an FTC staff member, COPPA and FTC's implementing regulations reflect various principles that are similar to the Fair Information Practice Principles.

FCC regulates the telecommunications industry pursuant to the Communications Act of 1934, as amended (Communications Act).[37] FCC follows the APA section 553 notice-and-comment rulemaking process to promulgate regulations implementing the Communications Act. FCC also has an enforcement bureau that pursues violations of its regulations and the Communications Act.

The Communications Act establishes separate definitions for "information services" and "telecommunications services" and treats these two types of services differently. Specifically, information services are subject to less regulation by FCC than telecommunications services under the

[32]COPPA also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under the age of 13.

[33]In addition to FTC, the attorney general of a state may also enforce COPPA under 15 U.S.C. § 6504(a) by bringing a civil action on behalf of the residents of the state if the attorney general has reason to believe that an interest of the residents of that state has been threatened or adversely affected by a violation of COPPA.

[34]Children's Online Privacy Protection Rule, 64 Fed. Reg. 22750 (Apr. 27, 1999).

[35]Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972 (Jan. 17, 2013).

[36]FTC's current COPPA regulations are set forth at 16 C.F.R. §§ 6501–6505.

[37]Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934), codified as amended at 47 U.S.C. §§ 151 *et seq*.

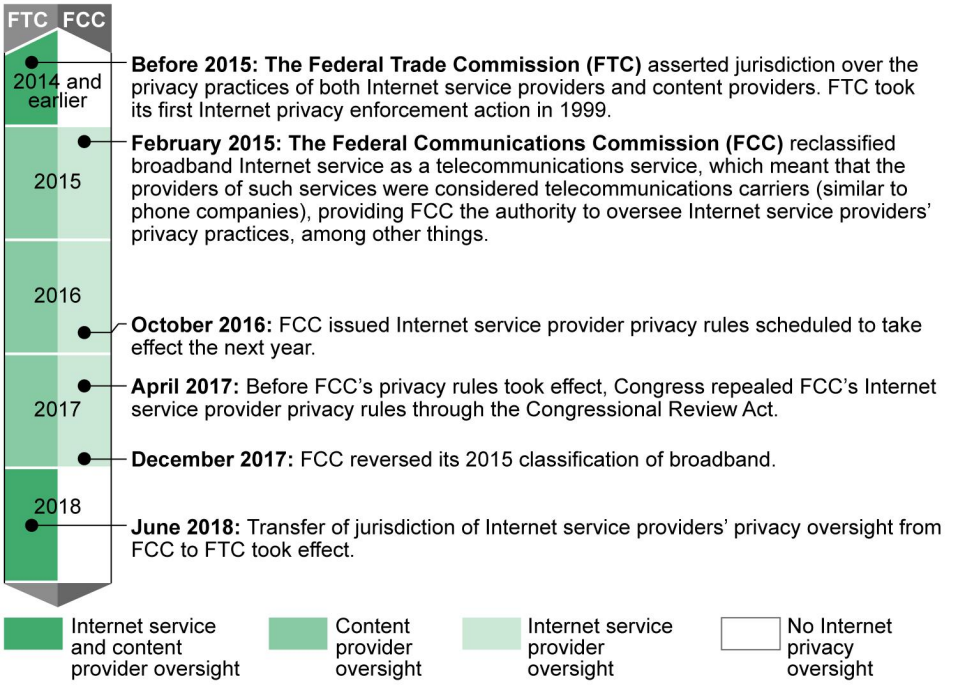
Communications Act.[38] However, FTC is prohibited from regulating telecommunications carriers (a provider of telecommunications services) under the common carrier exemption. Prior to 2015, Internet services were considered information services under the Communications Act, and thus FTC was not prohibited from considering the privacy practices of Internet service providers under its FTC Act authority to protect consumers from unfair and deceptive practices. This changed in 2015 when FCC classified broadband as a telecommunications service, which meant that broadband Internet service providers were considered telecommunications carriers and FCC asserted primary oversight over them. As a result of the reclassification, FTC no longer had jurisdiction over Internet service providers. Once FCC had asserted primary oversight over Internet service providers, FCC promulgated privacy regulations specific to them. However, before the privacy regulations went into effect, Congress repealed them under the Congressional Review Act.[39] In December 2017, FCC reclassified broadband as an information service—reverting Internet service providers' classification to what it had been prior to 2015. When that reclassification became effective in June 2018, jurisdiction of Internet privacy for Internet service providers was effectively transferred from FCC back to FTC. As a result, FCC currently has limited Internet privacy oversight responsibilities, as shown in figure 1.[40]

[38]A telecommunications carrier is regulated as a common carrier under Title II of the Communications Act and must provide nondiscriminatory access and is subject to price regulation, among other requirements. On the other hand, FCC has limited authority to regulate information service providers, while section 5 of the FTC Act specifically prohibits FTC from regulating common carriers.

[39]Under the Congressional Review Act, Congress may prevent a rule that is issued by a federal agency from taking effect or continuing in effect. 5 U.S.C. § 802(b)(1).

[40]In 2010, FCC promulgated a "transparency" rule that required a broadband Internet service provider to publicly disclose the commercial terms of its services, including its privacy policies, among other disclosures. FCC has retained the 2010 transparency rule with modifications.

**Figure 1: Timeline of FCC's and FTC's Internet Privacy Oversight**




Source: GAO analysis. | GAO-19-52

Note: Internet content providers are companies that provide various types of Internet-based services, such as social media, streaming media, search, navigation, and online shopping, among many others. Internet service providers are companies that provide access to the Internet.

# Stakeholders' Views Varied on the Benefits and Concerns with Collecting and Using Consumers' Data from the Internet

Perspectives on the benefits of and concerns about the collection and use of consumers' data from the Internet varied somewhat across stakeholder groups. Various stakeholders we interviewed—including those from academia, industry, and government—said that there should be a balance between the freedom of companies to collect and use consumers' data needed to provide services and the necessity to protect consumers' privacy. In general, industry stakeholders highlighted the benefits of data collection and use, such as facilitating innovation, while consumer advocacy groups and other stakeholders emphasized concerns about consumers' loss of control over their data and their lack of understanding of how companies collect and use their information.

Additionally, surveys and other literature that we reviewed on Internet privacy highlighted concerns among consumers. The key benefits of information collection were identified as:

- **Enables certain services.** According to two industry stakeholders, the collection and use of consumer data from the Internet enable content providers to provide services. These stakeholders said that sometimes a content provider must collect and use information from consumers to provide the service. For example, a mapping service must collect and use consumers' current location to provide them with up-to-date directions.
- **Provides low-cost or free services.** A representative from a content provider said that revenue from targeted advertising helps allow some content providers' services to be offered to consumers at little or no charge. Instead of charging a subscription fee, a social media company may be able to provide free service because it uses information that it collects from consumers to target advertisements to users on a customized, user-by-user basis. These ads are targeted to users based on interests they express through their use of social media, among other things. According to a representative from an Internet search engine, using consumer data for targeted advertising may be relatively less important for some kinds of content providers, such as search engines. This company representative said that search engines may use keywords entered for a particular Internet search to provide advertisements relevant to the search. For example, a search for "car insurance" can offer the consumer advertisements from car insurance companies without any additional data from the consumer other than the search's keywords.
- **Supports innovation and customization.** According to some stakeholders, the collection and use of data also benefit consumers through other means such as providing innovative products or customized services. According to a representative from a content provider, the collection of personal information, with consent, for commercial purposes can at times have benefits. The representative said, for example, that collection of images containing identifiable information, like faces, can help in the development of new technologies such as object and facial recognition. According to two content providers, consumers may also benefit from customized services and content. For example, according to a representative from a travel-related company, that company can collect information about a consumer to suggest travel itineraries and suggestions for activities. Additionally, representatives from a consumer advocacy group and a content provider stated that direct-marketing approaches are enabled

through data collection. Such marketing approaches allow consumers to receive advertisements that are uniquely tailored to their interests. For example, a consumer that a content provider has identified as being a hiker may receive advertisements for hiking boots.

Despite these benefits, public opinion surveys have shown concerns about the collection and use of consumers' information on the Internet. For instance, recent analyses based on surveys by the Pew Research Center[41] and NTIA showed that the public lacks trust in Internet privacy, a concern that may limit economic activities. NTIA's survey results show that privacy concerns may lead to lower levels of economic productivity as people decline to make financial transactions on the Internet. According to the NTIA analysis, in 2017, 24 percent of American households surveyed avoided making financial transactions on the Internet due to privacy or security concerns.[42] Consumers NTIA 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. Stakeholders we interviewed elaborated on some of these concerns:

- **Public disclosure and data breaches.** Some stakeholders, including representatives from content providers, said that personal information from the Internet can be publicly disclosed, including through data breaches. An academic and a former FCC commissioner told us that such disclosures are becoming more frequent. Various consumer advocacy groups and state governments continue to report data breaches. This personal information can include financial information such as credit card information, the disclosure of which can result in financial harm to the consumer. It can also include other kinds of sensitive information such as political views or medical conditions, the disclosure of which can cause non-financial harms such as embarrassment or harassment. According to public reports, the 2017 breach of consumer information from Equifax, a credit-reporting agency, resulted in the disclosure of 143 million American consumers' sensitive information. According to NTIA's 2017 survey, 45 percent of households surveyed reported major concerns about credit card

[41]Pew Research Center, *The State of Privacy in Post-Snowden America* (Washington, D.C.: Sept. 21, 2016).

[42]NTIA, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds* (Washington, D.C.: Aug. 20, 2018).

fraud. Regarding non-financial information, in a recent case FTC alleged that an Internet-based company publicly disclosed patients' sensitive medical information without their knowledge after patients submitted what they thought were confidential reviews of physicians. According to FTC, these reviews were then publicly posted on the company's website.

- **Financial and other harms.** Stakeholders identified both potential financial and non-financial harms associated with misuse of personal information from the Internet. A former FTC acting chair has said that privacy and data-security incidents can cause injuries that do not only involve financial loss and that it may be difficult to measure this type of non-financial injury. In a February 2018 speech, this former acting FTC chair cited a case that the agency filed involving the misuse of personal information from the Internet that resulted in people losing jobs or job opportunities or being threatened, stalked, and harassed. The acting chair said that in another case, there was evidence that several people committed suicide after their names and other data were disclosed. The commission can, by bringing suit in district court, obtain an order compelling content providers to provide monetary relief to consumers if a data disclosure results in financial harm to a consumer.[43] However, an academic noted that many data disclosures of sensitive information cannot be financially redressed; information can indefinitely persist on the Internet once it is disclosed.
- **Consumers' lack of understanding.** A range of stakeholders we interviewed, including those from industry, said that consumers lack an understanding of how their data are collected and used. Some stakeholders said content providers are insufficiently transparent about how they collect and use data. For instance, content providers' privacy policies, according to various stakeholders, may contain technical language that is difficult for typical consumers to understand, may be located in a difficult-to-access or inconspicuous part of the content provider's website, or may be lengthy to the point where it becomes prohibitively difficult for a consumer to set aside enough time to read. Furthermore, according to an academic, companies may have an incentive to intentionally obscure their privacy practices, since clarity could put the companies at a competitive disadvantage.

  The academic also stated that different privacy policies may apply to different parts of a consumer's experience on a single website. For

[43]This includes the FTC enforcement actions in appendix II involving monetary relief that were not in direct violation of the COPPA regulations.

example, the academic described how a website may have contracts with third-party vendors for specific services included on the website that consumers use, such as an online shopping cart's features. The privacy policy for the website and the third-party shopping cart can be separate and unrelated to each other, and consumers may not be aware of this since these policies may never appear to consumers or be hard to obtain. A representative from a consumer advocacy group also mentioned that consumers may be unaware that companies track consumers' Internet activity in order to target those consumers with customized prices. An academic said that these practices may disproportionately affect people with low computer literacy, as they may not be aware of tracking or know of ways to counteract it. In 2015, we found that the lack of computer and Internet skills is one of the primary barriers people face in using the Internet and that this is a particular problem for certain demographic segments who may lack exposure to or knowledge about computers, such as those of age 65 and older and those with low levels of income and education.[44]

- **Consumer lack of control.** Some academics and consumer advocacy groups also identified a lack of control as a concern with respect to Internet privacy—consumers have little or no control over how their information is collected, used, and shared. In a 2015 survey conducted by Pew Research Center, 65 percent of respondents said it is very important to be in control of what information is collected about them. However, according to an academic and a consumer advocacy group we interviewed, privacy policies offer consumers little or no bargaining power, and consumers may be forced to either accept the terms of the policy as written or not use the application or service at all. Furthermore, we recently reported that sometimes consumers' information is used for purposes that are altogether separate from what those consumers originally anticipated.[45] For example, FTC alleged in an enforcement action that in 2009 and 2010, a company told consumers that it would track the websites they visited in order to provide them with personalized offers, when in fact the company was also transmitting credit card information it collected through such tracking to third parties. The company settled with FTC. We also recently reported on how devices that comprise the Internet of Things pose privacy concerns for consumers, including that information

[44]GAO-15-473.

[45]GAO, *Internet of Things: Status and Implications of an Increasingly Connected World,* GAO-17-75 (Washington, D.C.: May 15, 2017).

collected by such Internet-connected devices can be used in ways to which the consumer was not given the option to opt out.[46]

As discussed above, stakeholders described various types of harm that could result from Internet privacy violations. Regardless of whether violations involve financial or other types of harm, a challenging factor in providing Internet privacy oversight is identifying the responsible parties. A former federal government official with experience in privacy issues said that it frequently is difficult to identify which Internet entity in the chain is ultimately responsible for a privacy-related harm. For example, if a consumer is harmed by the theft of his or her Social Security number, it can be difficult to determine which entity is responsible if multiple entities have suffered data breaches of information systems that contained the Social Security number. In addition to the challenges in identifying responsible parties, the federal government has faced challenges in providing Internet privacy oversight. Our prior work has found that such efforts lack clearly defined roles,[47] goals and performance measures,[48] and that gaps exist in the current privacy framework.[49]

[46]GAO-17-75.

[47]GAO-17-656.

[48]GAO-12-903.

[49]GAO-13-663.

# FTC and FCC Have Used Different Approaches to Oversee Internet Privacy

## FTC Primarily Uses Settlement Agreements with a Range of Companies to Address Internet Privacy Violations

We found that during the last decade, FTC filed 101 Internet privacy enforcement actions for practices that the agency alleged were unfair, deceptive, a violation of COPPA,[50] a violation of a settlement agreement, or a combination of those reasons.[51] Most of these actions pertained to first-time violations of the FTC Act for which FTC does not have the authority to levy civil penalties. In those cases where a party violated an FTC regulation or settlement agreement, however, FTC does have the authority to impose civil penalties. The 101 cases—filed between July 1, 2008 and June 30, 2018—involved a variety of products, services, and industries that collect and use personal information from the Internet. During the years for which we examined full-year data, the number of enforcement actions taken per year ranged from 5 in 2010 and 2016 to 23 in 2015. For example, in recent years, FTC took enforcement action against the following entities for alleged conduct that the agency contended violated section 5 or COPPA:

- a toy manufacturer for collecting personal information from children online without providing direct notice and obtaining their parents' consent;
- a computer manufacturer for pre-loading laptops with software that compromised security protections in order to deliver ads to consumers;
- a mobile ride-hailing business for misrepresenting the extent to which it monitored its employees' access to personal information about users;

[50]This includes violations of the COPPA statute as well as FTC's COPPA regulations.

[51]FTC settled its first Internet privacy case in 1999. We focused on FTC's enforcement cases filed over the last 10 years because of rapidly changing business models and technology in the Internet industry.

- a television manufacturer for installing software on its televisions to collect viewing data on 11 million consumers without their knowledge or consent and providing the viewing data to third parties; and
- a mobile advertising network for deceptively tracking the locations of hundreds of millions of consumers, including children, without their knowledge or consent, to serve them geographically targeted advertising.

Of the 101 actions filed during the 10-year period, 51 involved Internet content providers, 21 involved software developers, 12 involved the sale of information or its use in advertising, 5 involved manufacturers, 1 involved an Internet service provider, and 11 involved a variety of different products, such as those provided by rent-to-own companies or certification services.[52] 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. FTC levied civil penalties against two of those companies for violating their settlement agreements.[53] Also during this 10-year period, FTC levied civil penalties against 15 companies (a total of $12.7 million) for alleged violations of the COPPA regulations. The COPPA civil penalties ranged from $50,000 to $4 million and the average amount was $847,333. FTC can also seek to compel companies to provide monetary relief to those they have harmed. During this time period, FTC levied civil penalties against companies for violations of consent decrees or ordered monetary relief to consumers from companies for a total of $136.1 million. These payment orders ranged from $200,000 to $104.5 million and the average amount was $17 million.[54]

In the majority of these 101 enforcement actions that FTC settled, FTC alleged that companies engaged in practices that were deceptive. Examples of the charges FTC brought include:

[52]Some of these companies provide more than one type of service. We categorized these companies by the type of service that was the subject of the enforcement actions.

[53]During this period FTC also investigated other possible Internet privacy violations that were closed without the agency taking enforcement action.

[54]This sum does not represent the amount of money that consumers actually received or that was forfeited to the U.S. Treasury. In some cases, including the payment order for $104.5 million, FTC suspended the judgment because of the defendants' inability to pay.

- "Deceptive practices" cases (61 cases): In 2016, FTC alleged that Turn, Inc., an Internet advertising company, continued to track the Internet activities of consumers for targeted advertising purposes after the company had made representations that it would stop doing so. According to FTC, the company led consumers to believe they could turn off such tracking when in fact they were unable to do so.
- "Unfair practices" cases (4 cases): In 2014, FTC alleged that LeapLab, a data broker, knowingly provided scammers with hundreds of thousands of consumers' sensitive personal information, including Social Security and bank account numbers.
- "Unfair and deceptive" practices cases (19 cases): In 2015, FTC alleged that Equiliv Investments, a software developer, lured consumers into downloading its "rewards" application, saying it would be free of malware, when the application's main purpose was actually to load the consumers' mobile phones with malicious software to mine virtual currencies for the developer.
- COPPA and COPPA regulations cases (6 cases):[55] In 2011, FTC alleged that Broken Thumbs Apps, a software developer, had collected information from Internet applications that the developer specifically targeted toward children under the age of 13. FTC's complaint stated that the company had, among other things, failed to provide notice of what information it collected and how it was used and also had failed to inform parents of these practices and receive their consent as COPPA required.
- Violation of settlement agreement cases (2 cases): In 2012, Google agreed to pay a $22.5 million civil penalty to settle FTC charges that it misrepresented to users of Apple's Safari Internet browser that Google would not place tracking cookies or provide targeted ads to those users, violating an earlier settlement agreement between the company and FTC.

In 14 of the 101 cases, FTC required companies to be audited by outside entities to monitor compliance with the terms of the settlement. The audit period ranged from 5 years to 20 years, with an average of 17.5 years.

As noted above, 2 of the 101 cases involved a violation of FTC settlement agreements. In addition, in March 2018, FTC announced that it is investigating whether Facebook's privacy practices violate a 2012

[55]COPPA was used in nine other cases that also involved deceptive practices.

Facebook settlement agreement with FTC. In the case that resulted in the 2012 settlement, FTC charged Facebook with deceiving consumers by telling them they could keep their information private, but then allowing it to be shared and made public.

Appendix II contains more detailed information about the 101 cases.

## FCC Developed Internet Privacy Rule for Internet Service Providers That Was Later Repealed

As stated earlier, in 2015, FCC classified broadband Internet service as a telecommunications service, placing primary oversight of broadband Internet service providers' privacy practices under FCC's jurisdiction instead of FTC's jurisdiction. In 2016, FCC filed a privacy enforcement action against a mobile Internet service provider, alleging, in part, violation of section 222 of the Communications Act and FCC's Open Internet Transparency Rule. Section 222 requires telecommunications carriers to protect the confidentiality of customers' proprietary information. In that case, FCC fined Verizon Wireless $1.4 million for failing to disclose that it was inserting "unique identifier headers," also called "perma-cookies" or "super cookies" (mobile web tracking cookies that users cannot remove), into customers' Internet traffic over its wireless network. Although the settlement was finalized during the 2015-2017 period when FCC had asserted jurisdiction over the privacy practices of Internet providers, the Verizon Wireless practices occurred prior to the classification of Internet service providers as telecommunications carriers. The investigation therefore did not rely upon FCC's subsequent assertion of authority over Internet service providers' privacy practices.[56]

In October 2016, after FCC had reclassified broadband as a telecommunications service, the commission issued Internet service provider privacy regulations, asserting its authority under section 222 of the Communications Act. In April 2017, however, Congress repealed

[56]Specifically, FCC's consent decree in the Verizon case cited the Communications Act section 222 obligation for carriers to protect customers' proprietary information and FCC's Open Internet Transparency Rule, which requires Internet service providers to disclose accurate information to consumers about network management practices, performance, and commercial terms related to broadband service. *See* 47 U.S.C. § 222; 47 C.F.R. § 8.3; *FCC Enforcement Advisory; Open Internet Transparency Rule; Broadband Providers Must Disclose Accurate Information to Protect Consumers*, Public Notice, 29 FCC Rcd 8606 (EB 2014).

these regulations under the Congressional Review Act before they took effect. In December 2017, FCC then reversed its 2015 classification of broadband, and oversight of broadband Internet service providers' privacy practices reverted to FTC once the decision took effect in June 2018. In explaining the December 2017 decision, FCC's new chair said that FTC's privacy oversight approach regarding Internet service providers—using its authority to protect consumers against unfair, deceptive, and anti-competitive practices—had worked well in the past and that this action would "put the nation's most experienced privacy cop back on the beat." Under FCC's new legal approach, it no longer asserts jurisdiction to take enforcement action against Internet service providers for privacy-related matters, including mobile Internet service providers. As part of FTC's resumption of Internet service provider oversight, FCC and FTC entered into a memorandum of understanding in December 2017 spelling out their roles and responsibilities regarding oversight of these companies. FTC staff said that they regularly communicate with FCC and have an agreement to share Internet privacy complaints.

# Selected Stakeholders Provided Various Views on the Effectiveness of Current Internet Privacy Oversight and How It Could be Enhanced

## Industry Stakeholders View Current Enforcement Approach as Providing Flexibility, While Consumer Stakeholders See Limitations with This Approach

As previously discussed, no federal statute comprehensively and specifically governs Internet privacy across all sectors. FTC oversees some aspects of Internet privacy by using its FTC Act section 5 authority to protect consumers from unfair and deceptive practices. FTC also uses its specific COPPA authority to police the collection and use of personal information from children by online services. Some industry representatives said that FTC's enforcement has been effective because the agency has expertise and experience in privacy issues and has the flexibility to take enforcement action on a case-by-case basis. In addition, a content provider said that FTC has taken enforcement actions against companies of various sizes in different sectors and has a powerful tool by being able to require companies to be audited by outside entities for up to 20 years.

Industry stakeholders we interviewed generally said that "direct enforcement" of a statute is preferable to promulgating and enforcing regulations implementing that statute (which constitutes enforcement of the statute as well). These stakeholders noted several key concerns they believe exist with regulatory versus statutory enforcement of Internet privacy:

- **Regulations can stifle innovation.** Two industry stakeholders said that regulations can hinder companies' ability to innovate. For example, representatives from an Internet service provider said that innovation can stop during the rulemaking process as the industry waits for the regulation to be finalized.
- **Regulations may create loopholes.** Representatives from an Internet industry group and a content provider said that regulations can also contain loopholes that can be legally exploited because imprecise language in a regulation may allow a company to legally engage in an action that was originally unforeseen by the regulator.
- **Regulations can become obsolete.** Several industry stakeholders said regulations also may become obsolete quickly because the Internet industry is rapidly changing. An Internet industry representative noted that there can be large shifts in the Internet industry from year to year, while it often takes an agency much longer than a year to adopt a rule. Industry stakeholders said the flexibility of FTC's approach allows FTC to adapt continuously to changing market conditions.
- **Rulemakings can be lengthy.** FCC officials said that in some cases, rulemakings can take a long time, especially when the issues are complex and there is no statutory deadline. Our previous work on rulemaking found that length of time required for the development and issuance of final rules varied both within and among agencies.[57]

Additionally, while some stakeholders suggested that regulations can clarify acceptable practices, other stakeholders, including from industry and academia, said that enforcement actions can send a similar message. According to both a representative from a content provider and an academic, enforcement actions such as settlement agreements, for

[57]GAO, *Federal Rulemaking: Improvements Needed to Monitoring and Evaluation of Rules Development as Well as to the Transparency of OMB Regulatory Reviews,* GAO-09-205 (Washington, D.C.: Apr. 20, 2009).

example, establish precedents that companies can follow, similar to the way that case law developed by courts provides guidance for companies.

Although some industry representatives we interviewed said that FTC's use of settlement agreements provides companies with guidance, certain trade associations took a different position in a recent case brought before the U.S. Court of Appeals for the Third Circuit, *FTC v. Wyndham Worldwide Corp. 799 F.3d 236 (3d Cir. 2015).* However, the court did not agree with the associations' arguments. The case involved an enforcement action against Wyndham Worldwide Corporation where FTC alleged that data security failures led to three data breaches at the company in less than 2 years. The court considered whether FTC could bring an enforcement case involving cybersecurity using FTC's section 5 "unfair practices" authority and, if so, whether Wyndham had "fair notice" that its specific cybersecurity practices could be deemed "unfair."[58] A group of companies and the U.S. Chamber of Commerce wrote a friend-of-the-court brief supporting Wyndham, criticizing FTC's "regulation-through-settlements" approach. The companies argued this approach subjects businesses to "vague, unknowable, and constantly changing data-security standards" and businesses often are unaware of the standards to which they are held until after they receive a notice of investigation from FTC, at which point they must settle or expend considerable resources fighting the agency.

The Third Circuit determined that the statute, combined with FTC's interpretive guidance and enforcement complaints, gave fair notice that Wyndham's actions could be deemed "unfair" under the FTC Act. The court noted that the FTC Act simply asks whether "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." The court continued, "While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis . . . that considers a number of relevant factors….Fair notice is satisfied here as long as the

**Potential Limits on Federal Trade Commission (FTC) Remedies**

[58]"Fair notice" of what conduct violates the law is required by the Due Process Clause of the U.S. Constitution.

A recently decided federal appeals court case illustrates potential limits on the remedies that FTC can order in an "unfair practices" enforcement proceeding. In this 2018 case, *LabMD, Inc. v. FTC, 891 F.3d 1286 (11th Cir. 2018),* the U.S. Court of Appeals for the Eleventh Circuit found that FTC could not direct a medical laboratory to create and implement wholesale data-security protective measures as a remedy to the laboratory's alleged unfair practices.

FTC had filed a complaint against LabMD 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. The commission found that LabMD's inadequate security constituted an unfair act or practice and ordered LabMD to take various actions, including establishing and maintaining a reasonable and comprehensive information security program.

On appeal, the Eleventh Circuit ruled that FTC's 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. FTC had argued that the FTC Act gives it broad discretion to prevent unfair or deceptive acts or practices that injure the general public and that FTC had spelled out standards for LabMD to craft a reasonable security program. The court ruled, however, that such a general approach would make it difficult for a reviewing court to determine if LabMD had complied with the order, in the event of a future FTC challenge.

Source: GAO analysis. | GAO-19-52

company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."[59]

A majority of non-industry stakeholders we interviewed identified limitations in the current Internet privacy oversight approach because they view regulations in conjunction with enforcement as being more effective. These stakeholders include all of the former FTC commissioners we interviewed, three of the four former FCC commissioners we interviewed, and representatives from consumer advocacy groups we interviewed. In addition, a former FCC commissioner said that the current Internet privacy oversight approach is limited in part because he viewed regulations applying equally to all players in the Internet ecosystem in conjunction with enforcement as being more effective. A representative from a consumer advocacy group also said that regulations in conjunction with enforcement are essential for effective privacy protection. Some of these stakeholders noted key ways that they believe Internet privacy regulations can provide clarity to industry and consumers, as well as fairness and flexibility in enforcement:

- **Regulations can provide clarity.** An Internet industry group representative said that various companies have favorable views of regulations because they can provide clear expectations about what actions are permissible. Similarly, a former congressional staff member with expertise on privacy issues said that some companies have favorable views of regulations because the regulations often provide clearer expectations about what the companies can do. FCC officials said that with respect to telephone privacy provisions of the Communications Act, the telephone industry wanted rules because it sought greater clarity about what it should be doing, what constituted a violation, how to comply, and what behaviors were acceptable.
- **Regulations may promote fairness.** Some other stakeholders discussed the ability of regulations to provide fairness. For example, a former federal enforcement official described regulations as creating a fair and consistent oversight regime across the entire industry in a way that case-by-case enforcement actions do not. Another former federal enforcement official said that regulations give companies fair

[59]*FTC v. Wyndham Worldwide Corp.,* 799 F.3d at 255-56 (citations omitted).

notice of what actions may be violations and thus help those companies avoid surprising or unexpected enforcement.[60]

- **Regulations can be flexible.** An academic said that by targeting behaviors and not specific technologies, regulations can be written in such a way that they do not become obsolete. An academic also said that regulations based on broad performance-standards principles can avoid being overly prescriptive.[61] FCC officials also noted that regulations can be amended to adapt to changes in technology often faster than new laws can be enacted. Furthermore, regulations determined to be obsolete can be repealed. FTC staff told us that the agency systematically reviews all of its regulations every 10 years, even though it is only legally required to review its most significant ones, and that the number of FTC regulations has decreased because the agency determined prior ones were obsolete. The Regulatory Flexibility Act requires federal agencies to analyze the effect of their regulations on small entities.[62]

- **Regulations can be a deterrent.** FCC officials said that rules can have a deterrent effect on bad practices in the industry or have a role in mitigating the negative effects of bad practices after they occur. They said, for example, that the practice of pretexting (improperly obtaining people's telephone records) was greatly curtailed by an FCC regulation prohibiting such practices. They also said that rules can foreclose arguments by companies claiming that because no rule was in place, they had no reasonable notice or awareness that they should behave in a particular way.

Consumer advocacy groups and other stakeholders, including some former FTC and FCC commissioners, had concerns about the efficacy of an enforcement approach such as FTC's approach to Internet privacy

[60]As noted above, however, in the *Wyndham* case, the Third Circuit rejected an industry argument that FTC did not give fair notice of what actions may be violations.

[61]In a 2017 report on agencies' regulatory designs and enforcement decisions, we reported that agency officials preferred "performance" designs that establish an outcome but allow flexibility in how to achieve it. Agency officials also stated that in some cases their objectives could require use of more prescriptive "design-based" regulations that specify a certain required technology or action. GAO, *Federal Regulations: Key Considerations for Agency Design and Enforcement Decisions,* GAO-18-22 (Washington, D.C.: Oct.19, 2017).

[62]Regulatory Flexibility Act, Pub. L. No. 96-354, 94 Stat. 1164 (1980) (codified as amended at 5 U.S.C. §§ 601-612).

oversight, which focuses on enforcing a statute rather than implementing regulations. They said that FTC's enforcement approach limits the ability of the agency to affect companies' behavior, and that any enforcement activity occurs after the violation, undesirable behavior, harm, or illegal action has already occurred.[63] A former federal enforcement official also said that regulations can prevent companies from engaging in bad practices in the first instance and thus have a preventive effect. A former FCC commissioner said that by the nature of a direct statutory-enforcement approach (as opposed to rulemaking), an agency would only address a harm after it has occurred. As discussed above, for example, data often cannot be removed from the Internet because copies of the data can exist among many bad actors, and it can be difficult to identify the entity responsible for unwanted disclosures. Therefore, it may be more important to avoid such Internet privacy harms from occurring in the first place. Another former FCC commissioner told us that Internet privacy oversight should be returned to FCC because it has APA section 553 notice-and-comment rulemaking authority and considerable enforcement experience.

Representatives from consumer advocacy groups said that FTC's enforcement action has been insufficient because it investigates only a small portion of actual Internet-privacy violations or takes action regarding only the most egregious or outrageous cases that it can win. FTC has also stated in its strategic plan that it focuses on investigating and litigating cases that cause or are likely to cause substantial injury to consumers and that by focusing on practices that are actually harming or likely to harm consumers, FTC can best use its limited resources.[64] Representatives from an Internet association said that FTC's Internet-privacy enforcement actions should focus on concrete harms. An FTC staff member from the Division of Privacy and Identity Protection said that the agency has been effective with the limited enforcement resources it has available. Furthermore, the staff member said the agency uses no formal written criteria or template to assess individual cases but considers the size and scale of a company's effect on consumer privacy when deciding whether to take enforcement action. However, a former FTC commissioner told us that the agency needs more resources to effectively oversee Internet privacy.

[63]FTC can seek an injunction in court to prevent future harm, however, and can bring cases where the public has not yet been injured. *See* 15 U.S.C. § 53.

[64]FTC, *Strategic Plan for Years 2018 to 2022*.

We asked stakeholders whether it was clear under what circumstances FTC will take Internet privacy enforcement action. In response, some stakeholders said that FTC's enforcement priorities are reflected in its settlement agreements, which provide information that is similar to a body of case law. Individual commissioners also may issue statements explaining their decisions. Two stakeholders also said that FTC's closing letters, which the agency sends to companies and posts on its website when it closes an investigation without taking enforcement action, may explain its decisions. Other stakeholders said that more guidance would be helpful to provide additional clarity on how the agency uses its Internet privacy enforcement authority. FTC staff and other stakeholders also said that FTC has provided useful Internet privacy guidance. For example, in 2015, FTC published guidance for businesses on complying with COPPA.

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

Various stakeholders we interviewed said that opportunities exist for enhancing Internet privacy oversight. A key component of FTC's mission, as specified by the FTC Act, is to protect consumers against unfair and deceptive practices. As discussed earlier, some stakeholders believe that FTC's reliance on its unfair and deceptive practices authority to address Internet privacy issues has limitations. In addition, although the Fair Information Practice Principles provide internationally recognized principles for protecting the privacy and security of personal information, they are not legal requirements and FTC cannot rely on them to define what constitutes unfair and deceptive practices related to privacy and data security.

We stated in our 2013 information resellers report that the current U.S. privacy framework is not always aligned with the Fair Information Practice Principles and that these principles provide a framework for balancing the need for privacy with other interests.[65] We found that there are limited privacy protections under federal law for consumer data used for marketing purposes. We said that although the Fair Information Practice Principles call for restraint in the collection and use of personal information, the scope of protections provided under current law has been narrow in relation to: (1) individuals' ability to access, control, and correct

[65]GAO-13-663.

their personal data; (2) collection methods and sources and types of consumer information collected; and (3) new technologies, such as tracking of web activity and the use of mobile devices. Although we recommended in that report that Congress consider strengthening the consumer privacy framework to reflect the effects of changes in technology and the marketplace, this matter for congressional consideration was not specific to Internet privacy or to the oversight authorities of any particular agency or agencies.

As noted above, various stakeholders expressed concern about the ability of consumers to control their data and understand how that data are used. These concerns suggest that companies are not always following the Fair Information Practice Principles, such as that companies' data practices should be transparent, allow consumers the right to access and edit their data, and limit the collection of data to the extent feasible.

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 statutory or regulatory violation.[66]

## Privacy Statute

Stakeholders from a variety of perspectives—including from academia, industry, consumer advocacy groups, and former FTC and FCC commissioners—told us that a privacy statute could enhance Internet privacy oversight by, for example, clearly articulating to consumers, industry, and privacy enforcers what behaviors are prohibited, among other things. In addition, a former FCC commissioner said that a new privacy statute could enhance Internet privacy oversight by creating uniform standards for all players in the Internet ecosystem that is focused on the consumer rather than the regulatory legacy of the companies involved (regulations that apply to specific types of companies based on

[66]As discussed later, some stakeholders said that FTC's Internet privacy enforcement could be more effective with authority to levy civil penalties for first-time violations of the FTC Act, the statute that gives FTC its general authority.

what they are or used to be, such as telecommunications carriers, cable companies, broadcasters, and mobile wireless providers). The former FCC commissioner said that as companies, technologies, and markets change, there is a question about whether existing law should be modernized. In 2015, FTC staff recommended that Congress enact broad-based legislation that is flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.[67] Some stakeholders suggested that such a framework could either designate an existing agency as responsible for privacy oversight (such as FTC) or create a new privacy-oriented agency. A representative from a consumer advocacy group mentioned that the European Union, for example, has established the European Data Protection Supervisor, an independent data protection authority, to monitor and ensure the protection of personal data and privacy. Similarly, 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 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 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 over exempted industries such as common carriers. In addition, a former FCC commissioner said that it is more difficult for FTC to take effective action because its enforcement comes only after a complaint and after an often lengthy review process. The former FCC commissioner also said that without "ex ante" rules (rules that define prohibited activity before it has occurred), there inevitably will be delay, confusion, and lack of knowledge about what is and is not acceptable behavior.

In addition, some stakeholders—including a representative from a consumer group, a former federal enforcement official, and a former FCC commissioner—said FTC's section 5 "unfair or deceptive practices"

[67]FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World* (January 2015).

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." For example, under section 5, FTC has charged companies with committing a "deceptive" practice if their privacy policies said they would not collect or use consumers' personal information but then did so. However, a former congressional staff member said that companies often write broad and vague policy statements, making it difficult for FTC to charge companies with committing deceptive practices. Instead, according to a representative from a consumer advocacy group, FTC would have to show the companies' actions were "unfair," which, according to the representative, is legally difficult to establish. We found in our 2017 report on vehicle data privacy that most automakers' written privacy notices used vague language.[68] Similarly, we found in our 2012 report on mobile device location data that although companies' policies stated that they shared location data with third parties, they were sometimes vague about which types of companies these were and why they were sharing the data.[69]

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 was confirmed in our analysis of FTC's Internet privacy enforcement actions discussed previously. However, a representative from a consumer advocacy group said that FTC's ability to take such action is limited practically to instances where a company violates its own privacy policy—companies generally can collect and use data in any way they want if they include language in their policies asserting their intent to do so.[70] According to a former FCC commissioner, a privacy statute could clarify the situations in which FTC could take enforcement action.

## 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-

[68]GAO-17-656.

[69]GAO-12-903.

[70]FTC has taken enforcement action for a deceptive trade practice not only when a company violates its own privacy policy but also, for example, when representations are made on blog posts by employees related to privacy, privacy-related representations in product manuals and other activities.

comment rulemaking authority. As discussed above, that provision lays out the basic process by which so-called informal agency rulemaking shall be conducted, namely, publication of proposed regulations in the *Federal Register*; an opportunity for public comment (written and possibly oral submission of data and views); and publication of final regulations in the *Federal Register* with an explanation of the rules' basis and purpose. Also as noted above, Congress imposed additional rulemaking steps on FTC in the Magnuson-Moss Act when FTC is promulgating rules under section 5 of the FTC Act. These additional steps include providing the public and certain congressional committees with advance notice of proposed rulemaking (in addition to 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. Finally, Congress made it easier for the public to appeal FTC's Magnuson-Moss rules by making the agency meet a higher standard when the rules are challenged in court. FTC staff said that these additional steps add time and complexity to the rulemaking process.

In congressional testimony in 2010, the then-Director of FTC's Bureau of Consumer Protection said that "if Congress enacts privacy legislation, the commission agrees that such legislation should provide APA rulemaking authority to the commission."[71] According to FTC, this testimony was voted on and approved by the commissioners and, therefore, constituted the commission's official position at the time.

Moreover, according to stakeholders, in many cases regulations can be used to implement statutes. Officials from other consumer and worker protection agencies we interviewed described their enforcement authorities and approaches. For example, officials from the CFPB and the FDA, both of which use APA section 553 notice-and-comment rulemaking, said that their rulemaking authority assists in their oversight approaches and works together with enforcement actions. OSHA officials said that the standards that the agency promulgates under its authority[72]

[71]David Vladeck, Director of the FTC Bureau of Consumer Protection, *Prepared Statement of the Federal Trade Commission on Consumer Privacy,* testimony before the House Committee on Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection, 111th Cong., 2nd Sess., July 22, 2010.

[72]Occupational Safety and Health Act of 1970 (OSH Act), Pub. L. No. 91, 596, 84 Stat. 1590 (1970).

specify what employers are required to do to reduce safety and health risks to workers. Such standards lay out the workplace conditions that must be maintained by employers and require that employers implement certain practices, operations, or processes that ensure worker protections.[73] EEOC officials said that regulations are used to guide investigations that establish whether enforcement action is appropriate. CPSC officials said that the agency conducts consumer protection not only by establishing and enforcing mandatory regulations, but also through collaborative actions such as educating industry, developing consensus voluntary safety standards, removing defective products from the marketplace through voluntary corrective actions, and litigating when necessary. In addition, in contrast to FTC's approach, FCC has APA section 553 notice-and-comment rulemaking authority and has issued regulations implementing section 222 of the Communications Act using that rulemaking authority to protect the privacy of telephone users.

### Ability to Levy Civil Penalties for Initial Violations and to Impose Larger Civil Penalties

Some stakeholders suggested that FTC's current ability to levy civil penalties could also be enhanced. Currently, FTC can levy civil penalties against companies for violating certain regulations, such as COPPA regulations, or if the company violates 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. Another academic noted, however, that fines may be relatively less effective in industries where there is limited competition[74] because the costs of those fines may be more effectively passed on to consumers in the form of higher prices for services. In addition, some stakeholders said that payments required by

[73]According to OSHA officials, unlike the general duty clause of the OSH Act, which broadly requires employers to maintain safe and healthful workplaces, regulatory standards address specific safety and health hazards, explicitly describe what employers must do to comply with the law, can be tailored to particular industries, and can be enforced more readily than the general duty clause.

[74]We found in 2017 that about half of Americans have access to only one fixed Internet service provider. GAO, *Broadband: Additional Stakeholder Input Could Inform FCC Actions to Promote Competition,* GAO-17-742 (Washington, D.C.: Sept. 19, 2017).

FTC orders are not large enough to act as a deterrent and that companies may consider them to be a cost of doing business.

There is a growing debate about the federal government's role in overseeing Internet privacy. In a July 2018 congressional hearing, FTC's new chair testified that the FTC Act cannot address all privacy and data-security concerns in the marketplace. The chair said, for example, that FTC's lack of civil penalty authority for violations of the FTC Act reduces its deterrent capability. He also noted the agency lacks authority over non-profits and over common carrier activity, even though those entities and activities often have serious implications for consumer privacy and data security.[75] In November 2018, FTC's chair testified before Congress and urged Congress to consider enacting privacy legislation that would be enforced by FTC.[76] A majority of the commission has indicated support for APA rulemaking and civil penalty authority for privacy. FTC also held hearings in September, November, and December 2018 to advance the discussion around privacy issues, among other topics, and FTC plans to hold an additional hearing on data security and consumer privacy in February 2019. In a *Federal Register* notice, FTC announced that it is interested in the benefits and costs of various state, federal and international privacy laws and regulations, including the potential conflicts

[75]Joseph Simons, Chair of the FTC, *Oversight of the Federal Trade Commission,* testimony before the House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection, 115th Cong., 2nd Sess., July 18, 2018. Legislation was introduced in the last Congress related to some of these topics. For example, Senators Markey and Blumenthal and Rep. McNerney introduced legislation that would provide FTC with APA notice-and-comment rulemaking authority to implement the bill's Internet privacy standards after consultation with the FCC. *See* MY DATA Act of 2017, S. 964, 115th Cong. (2017); MY DATA Act of 2017, H.R. 2356, 115th Cong. (2017). Similar legislation, introduced by Sen. Leahy and Rep. Cicilline, would direct FTC to implement specific standards set by Congress, using APA rulemaking, to require certain companies to safeguard sensitive personally identifiable information. The bill would also give FTC civil penalty authority under the FTC Act to enforce the requirements of the bill. *See* Consumer Privacy Protection Act of 2017, S. 2124, 115th Cong. (2017); Consumer Privacy Protection Act of 2017, H.R. 4081, 115th Cong. (2017). The Secure and Protect Americans' Data Act, introduced last Congress by Rep. Schakowsky and co-sponsored by Rep. Pallone, would direct FTC to promulgate regulations implementing specific legislative standards using APA rulemaking procedures in order to require information brokers to provide consumers with access to information. *See* The Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. (2017).

[76]*See* Prepared Statement of the Federal Trade Commission, testimony before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security, 115th Cong., 2nd Sess., Nov. 27, 2018.

among those standards.[77] FTC also indicated that it is particularly interested in the efficacy of the commission's use of its current authority and the identification of any additional tools or authorities the commission may need to adequately deter unfair and deceptive conduct related to privacy and data security. Also in July 2018, an NTIA official announced that NTIA, in coordination with the Commerce Department's International Trade Administration and National Institute of Standards and Technology, had recently started holding stakeholder meetings to identify common ground and formulate core, high-level principles on data privacy.

Regarding the development of the Administration's approach to consumer privacy, in September 2018, NTIA requested comments on ways to advance consumer privacy while protecting prosperity and innovation. Our 2009 report on a framework for assessing proposals for modernizing the financial regulatory system similarly found that regulators should have the authority to carry out and enforce their statutory missions.[78] We further said that a regulatory system should be flexible and forward looking, allowing regulators to readily adapt to market innovations and changes, including identifying and acting on emerging risks in a timely way without hindering innovation. These factors are useful considerations as the federal government explores how it can better oversee privacy and data security. Having sufficient and appropriate authorities and providing flexibility to address a rapidly evolving Internet environment could better ensure that the federal government can protect consumers' privacy.

# Conclusions

Recent developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider comprehensive Internet privacy legislation. Although 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, there is no comprehensive federal privacy statute with specific standards. Debate over such a statute could provide a vehicle for consideration of the Fair Information Practice Principles, which are intended to balance privacy concerns with the need for using consumers'

[77] *See* Hearings on Competition and Consumer Protection in the 21st Century, 83 Fed. Reg. 38307 (Aug. 6, 2018).

[78] GAO-09-216.

data. Such a law could also empower a specific agency or agencies to provide oversight through means such as APA section 553 rulemaking, civil penalties for first time violations of a statute, and other enforcement tools. Comprehensive legislation addressing Internet privacy that establishes specific standards and includes APA notice-and-comment rulemaking and first-time violation civil penalty authorities could help 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.

## Matter for Congressional Consideration

Congress should 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.

## Agency Comments

We provided a draft of this report to FTC, FCC, and the Department of Commerce for their review and comment. FTC and FCC provided technical comments, which we incorporated as appropriate. The Department of Commerce indicated that it did not have comments.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the FTC chair, the FCC chair, the Secretary of Commerce, and interested congressional committees. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or members of your staff have any questions about this report, 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 report. Major contributors to this report are listed in appendix III.

Sincerely yours,

Alicia Puente Cackley
Director, Financial Markets and Community Investment

Mark L. Goldstein
Director, Physical Infrastructure Issues

# Appendix I: Interviewees

For this review, we interviewed staff from agencies with roles in Internet privacy; officials from other consumer- and worker-protection agencies; stakeholders from consumer advocacy groups, industry groups, Internet service providers, and Internet content providers; academics; and former government officials. To obtain a variety of perspectives, we selected Internet service providers that represented different industry sectors and Internet content providers that provide a variety of information and social media services. Academic stakeholders were selected because of their expertise in privacy, consumer protection, and regulatory issues. We also interviewed former Federal Trade Commission (FTC) and Federal Communications Commission (FCC) commissioners who served during the Barack Obama and George W. Bush administrations and are from different political parties.

## Academics

Alessandro Acquisti, Professor of Information Technology and Public Policy, Carnegie Mellon University
Howard Beales, Professor of Strategic Management and Public Policy, The George Washington University[1]
Christian Catalini, Associate Professor of Technological Innovation, Entrepreneurship, and Strategic Management, Massachusetts Institute of Technology
Chris Hoofnagle, Adjunct Professor of Law, University of California Berkeley
Ginger Zhe Jin, Professor of Economics, University of Maryland[2]
Jane Kirtley, Professor of Media Ethics and Law, University of Minnesota
Jeffrey Lubbers, Professor of Practice in Administrative Law, American University
Tejas Narechania, Assistant Professor of Law, University of California Berkeley
Daniel Solove, Professor of Law, The George Washington University
Peter Swire, Professor of Law and Ethics, Georgia Institute of Technology

[1]Former director of FTC's Bureau of Consumer Protection.

[2]Former director of FTC's Bureau of Economics.

David Vladeck, Professor of Law, Georgetown University[3]

## Consumer advocacy groups

Center for Democracy and Technology
Center for Digital Democracy
Consumer Federation of America
Public Knowledge

## Federal government agencies

Consumer Financial Protection Bureau (CFPB)
Consumer Product Safety Commission (CPSC)
Department of Commerce, National Telecommunications and Information Administration (NTIA)
Equal Employment Opportunity Commission (EEOC)
Federal Communications Commission (FCC)
Federal Trade Commission (FTC)
Food and Drug Administration (FDA)
Occupational Safety and Health Administration (OSHA)

## Former government officials

Kathleen Abernathy, former FCC commissioner
Anthony Alexis, former head, CFPB Office of Enforcement
Julie Brill, former FTC commissioner
Michael Copps, former FCC commissioner and acting chair
Robert Gellman, former chief counsel, Subcommittee on Information, Justice, Transportation, and Agriculture, Committee on Government Operations, U.S. House of Representatives
William Kovacic, former FTC commissioner and chair
Travis LeBlanc, former chief, FCC Enforcement Bureau
Jon Leibowitz, former FTC commissioner and chair
Robert McDowell, former FCC commissioner
Deborah Platt Majoras, former FTC chair
Tom Wheeler, former FCC chair

[3]Former director of FTC's Bureau of Consumer Protection.

## Industry groups

Internet Association
NCTA - The Internet & Television Association
USTelecom - The Broadband Association
WTA - Advocates for Rural Broadband

## Internet content providers

Apple
Discovery
DuckDuckGo
Facebook
Google
TripAdvisor

## Internet service providers

Advanced Communications Technology
Charter Communications
Comcast
HughesNet
MTE Communications
Verizon

# Appendix II: Federal Trade Commission Internet Privacy Enforcement Cases

The following table identifies 101 Federal Trade Commission (FTC) Internet privacy enforcement actions filed between July 1, 2008 and June 30, 2018 in which the agency alleged a violation of either the Federal Trade Commission Act (FTC Act) or the Children's Online Privacy Protection Act (COPPA) and implementing COPPA regulations and subsequently entered into a settlement agreement with the target entity. Although some of these cases may involve both Internet data privacy and security issues, this table does not include cases that involved data security issues only.

**Table 2: FTC's Internet Privacy Enforcement Cases Filed between July 1, 2008 and June 30, 2018**

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Uber Technologies | Deceived consumers about employee access to consumer personal information. | Pending (FTC is seeking to revise the settlement)[a] | Deceptive | Pending |
| My Ex | Posted intimate images of people without their consent. | 6/15/2018 | Unfair | $2,022,930 (default judgment) |
| PayPal | Misled consumers about privacy of financial transactions. | 5/23/2018 | Deceptive | 10 years |
| Prime Sites (Explore Talent) | Collected information from children under the age of 13 without providing notice or obtaining consent from the children's parents. | 2/12/2018 | COPPA | $500,000 |
| VTech Electronics Limited and VTech Electronics North America | Collected information from children under the age of 13 without providing notice or obtaining consent from the children's parents. | 1/8/2018 | COPPA and deceptive | $650,000 and 20 years |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Lenovo | Unfairly pre-installed advertising software on consumers' laptops that collected sensitive information that caused or likely caused injury. | 1/2/2018 | Unfair and deceptive | 20 years |
| Decusoft | Deceived consumers about participation in international privacy program. | 11/20/2017 | Deceptive | no evidence found |
| TCPrinting.net | Deceived consumers about participation in international privacy program. | 11/20/2017 | Deceptive | no evidence found |
| Md7 | Deceived consumers about participation in international privacy program. | 11/20/2017 | Deceptive | no evidence found |
| Blue Global | Unfairly sold information to entities whose security practices the respondent failed to verify and deceptively made false and misleading representations to consumers. | 7/5/2017 | Unfair and deceptive | $104,470,817 |
| SpyChatter | Deceived consumers about participation in international privacy program. | 4/12/2017 | Deceptive | no evidence found |
| Turn | Deceptively tracked consumers after consumers attempted to prevent such tracking. | 4/6/2017 | Deceptive | no evidence found |
| Sentinel Labs | Deceived consumers about participation in international privacy program. | 3/29/2017 | Deceptive | no evidence found |
| Vir2us | Deceived consumers about participation in international privacy program. | 3/29/2017 | Deceptive | no evidence found |
| Upromise (violation of a settlement agreement) | Continued to deceive consumers about the extent Upromise collected information from them, violating the terms of a prior FTC order. | 3/23/2017 | Settlement agreement violation | $500,000 |
| Vizio | Tracked consumers' television viewing without consumers' knowledge or consent. | 2/6/2017 | Unfair and deceptive | $1,500,000 and 20 years |
| Practice Fusion | Failed to disclose that users' reviews of doctors, some of which contained sensitive information, would be publicly posted. | 8/15/2016 | Deceptive | no evidence found |
| Very Incognito Technologies (Vipvape) | Deceived consumers about participation in international privacy program. | 6/29/2016 | Deceptive | no evidence found |
| InMobi | Deceptively tracked the physical location of millions of consumers for advertising purposes without their consent. | 6/22/2016 | COPPA and deceptive | $4,000,000 and 20 years |
| General Workings (Vulcan) | Unfairly replaced consumers' video game with software that installed respondent's own applications on consumers' devices. | 4/18/2016 | Unfair and deceptive | no evidence found |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Sitesearch Corp. (LeapLab) | Unfairly collected and sold hundreds of thousands of consumers' loan applications, which included sensitive information such as Social Security numbers, to entities without legitimate business needs for such information. | 2/5/2016 | Unfair | $4,124,710 |
| Craig Brittain | Deceptively acquired and posted intimate images of people. These people were told they would have to pay to remove such images. | 12/28/2015 | Unfair and deceptive | no evidence found |
| Retro Dreamer | Collected information from children under the age of 13 without providing notice or obtaining consent from the children's parents. | 12/17/2015 | COPPA | $300,000 |
| LAI Systems | Collected information from children under the age of 13 without providing notice or obtaining consent from the children's parents. | 12/17/2015 | COPPA | $60,000 |
| Forensics Consulting Solutions | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Contract Logix | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| SteriMed Medical Waste Solutions | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Pinger | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| One Industries | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| NAICS Association | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Just Bagels Manufacturing | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Jubilant Clinsys | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| IOActive | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Inbox Group | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Golf Connect | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Dale Jarrett Racing Adventure | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| California Skate-Line | Deceived consumers about participation in international privacy program. | 9/29/2015 | Deceptive | no evidence found |
| Nomi Technologies | Tracked consumers' movements throughout stores without their consent and without the option to opt-out. | 8/28/2015 | Deceptive | no evidence found |
| TES Franchising | Deceived consumers about participation in international privacy program. | 5/20/2015 | Deceptive | no evidence found |
| American International Mailing | Deceived consumers about participation in international privacy program. | 5/20/2015 | Deceptive | no evidence found |
| Equiliv Investments | Deceptively included virtual currency mining software on apps that were marketed to consumers as being for other purposes. | 4/23/2015 | Unfair and deceptive | no evidence found |
| Jerk | Lied to consumers about their ability to edit personal information about them that the respondent had publicly posted. | 3/13/2015 | Deceptive | (motion for summary decision) no evidence found |
| True Ultimate Standards Everywhere | Respondent misrepresented that it had validated the privacy practices of websites it provided certifications for. | 3/12/2015 | Deceptive | $200,000 and 10 years |
| PaymentsMD | Respondent did not adequately inform consumers that it was collecting their medical information. | 1/27/2015 | Deceptive | no evidence found |
| Snapchat | Misrepresented the extent to which consumers' messages would be impermanent and deceived consumers over the amount of personal data collected. | 12/23/2014 | Deceptive | 20 years |
| Yelp | Allowed children under the age of 13 to register on its website. Failed to adequately test its services to ensure such children did not register. | 9/16/2014 | COPPA | $450,000 |
| TinyCo | Offered extra points in video games to children under the age of 13 in exchange for their email addresses in violation of the necessary steps required for the collection of children's personal information. | 9/16/2014 | COPPA | $300,000 |
| BitTorrent | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Apperian | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Atlanta Falcons Football Club | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Baker Tilly Virchow Krause | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Charles River Laboratories, Int'l | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| DataMotion | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| DNA Diagnostics Center | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Denver Broncos Football Club | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Fantage.com | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Level 3 Communications | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Reynolds Consumer Products | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Receivable Management Services Corporation | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| Tennessee Football | Deceived consumers about participation in international privacy program. | 6/19/2014 | Deceptive | no evidence found |
| American Apparel | Deceived consumers about participation in international privacy program. | 6/16/2014 | Deceptive | no evidence found |
| Aaron's | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/10/2014 | Unfair | no evidence found |
| Goldenshores Technologies | Flashlight app deceptively sent physical location and other information to third party advertisers, among others. | 3/31/2014 | Deceptive | no evidence found |
| Aspen Way Enterprises | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| B. Stamper Enterprises | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| C.A.L.M. Ventures | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| J.A.G. Rents | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| Red Zone Investment Group, Inc. | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| Showplace | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| Watershed Development Corp. | Unfairly placed software on computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| DesignerWare | Unfairly developed software for computers rented by customers that monitored them, took screenshots of sensitive information, and used the computers' cameras to photograph them as well. | 4/11/2013 | Unfair and deceptive | no evidence found |
| EPIC Marketplace | Respondent deceptively reviewed consumers' Internet browsing history as part of its advertising efforts. | 3/13/2013 | Deceptive | no evidence found |
| Compete | Misled consumers about the extent to which its software tracked and collected their personal information. | 2/20/2013 | Unfair and deceptive | 20 years |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Path | Deceptively collected information from consumers' mobile device address books, including information about children. | 2/8/2013 | COPPA and deceptive | $800,000 and 20 years |
| Google (violation of settlement agreement) | Misrepresented to consumers that default settings would block Google's advertising trackers on a particular Internet browser. | 11/16/2012 | Settlement agreement violation | $22,500,000 |
| Direct Lending | Unfairly sold sensitive information to entities that targeted vulnerable consumers. | 10/11/2012 | Unfair | no evidence found |
| Artist Arena | Collected children's personal information without prior parental consent and activated a child's registration without parental consent | 10/3/2012 | COPPA and deceptive | $1,000,000 |
| Myspace | Respondent violated its own privacy policy by allowing advertisers access to consumers' personal information. | 8/30/2012 | Deceptive | 20 years |
| Facebook | Represented to consumers that information could be kept private when in fact it was repeatedly made public. | 7/27/2012 | Unfair and deceptive | 20 years |
| RockYou Inc. | Knowingly collected information from children without parental consent. | 3/28/2012 | COPPA and deceptive | $250,000 |
| Upromise | Deceptively collected more information from consumers than the respondent adequately disclosed and unfairly failed to protect consumer information. | 3/27/2012 | Unfair and deceptive | 20 years |
| skidekids | Collected personal information from children without obtaining prior parental consent. | 2/1/2012 | COPPA and deceptive | $100,000 and 5 years |
| ScanScout | Deceived consumers that they could opt-out of receiving targeted advertising when in fact they could not. | 12/14/2011 | Deceptive | no evidence found |
| Google | Used deceptive practices and violated their own privacy policy when starting a social network. | 10/13/2011 | Deceptive | 20 years |
| FrostWire | Developed software that misled consumers and likely caused consumers to expose sensitive information. | 10/12/2011 | Unfair and deceptive | no evidence found |
| Broken Thumbs Apps | Collected and disclosed personal information from children without obtaining prior parental consent. | 9/8/2011 | COPPA | $50,000 |

| Respondent(s) | Summary of privacy allegations | Date of FTC settlement | Type of FTC allegation (COPPA, unfair or deceptive practice, violation of consent order) | Civil penalty or monetary relief to consumers proposed by FTC and/or independent audit duration |
|---|---|---|---|---|
| Chitika | Respondent deceived consumers about how the opt-out mechanism of its tracking activities functioned. Opt-out choices expired after 10 days. | 6/7/2011 | Deceptive | no evidence found |
| Playdom Inc. | Collected and disclosed personal information from children without obtaining prior parental consent. | 5/24/2011 | COPPA and deceptive | $3,000,000 |
| US Search | Deceived consumers that they could pay to prevent third parties from accessing information about them. | 4/14/2011 | Deceptive | no evidence found |
| EchoMetrix | Collected and disclosed personal information from children without obtaining prior parental consent. | 11/30/2010 | Deceptive | no evidence found |
| CyberSpy Software | Sold key logging software that unfairly allowed clients to secretly monitor unsuspecting consumers' computer activity. | 4/22/2010 | Unfair and deceptive | no evidence found |
| Control Scan | Respondent misrepresented that it had validated the privacy practices of websites it provided certifications for. | 4/8/2010 | Deceptive | $750,000 |
| Directors Desk | Deceived consumers about participation in international privacy program. | 1/12/2010 | Deceptive | no evidence found |
| World Innovators | Deceived consumers about participation in international privacy program. | 1/12/2010 | Deceptive | no evidence found |
| Collectify | Deceived consumers about participation in international privacy program. | 11/9/2009 | Deceptive | no evidence found |
| Progressive Gaitways | Deceived consumers about participation in international privacy program. | 11/9/2009 | Deceptive | no evidence found |
| Onyx Graphics | Deceived consumers about participation in international privacy program. | 11/9/2009 | Deceptive | no evidence found |
| ExpatEdge Partners | Deceived consumers about participation in international privacy program. | 11/9/2009 | Deceptive | no evidence found |
| Iconix Brand Group | Collected personal information from children without obtaining prior parental consent. | 11/5/2009 | COPPA and deceptive | $250,000 |
| Sears Holdings Management Corporation | Deceived consumers about the extent to which respondent collected information about them. | 8/31/2009 | Deceptive | no evidence found |
| Sony BMG Music Entertainment | Collected and disclosed personal information from children without obtaining prior parental consent. | 12/15/2008 | COPPA and deceptive | $1,000,000 |

Legend: — = no evidence of proposed fine, restitution, or audit found for this case

Source: GAO analysis of FTC enforcement cases. | GAO-19-52

Note: For the purposes of this chart, we have only included FTC's role in these cases.

[a]Uber Technologies previously settled with respect to its open case. However, FTC discovered additional information related to the case and is seeking to revise the original settlement.

# Appendix III: GAO Contacts and Staff Acknowledgments

## GAO Contacts

Alicia Puente Cackley, (202) 512-8678 or cackleya@gao.gov
Mark Goldstein, (202) 512-2834 or goldsteinm@gao.gov

## Staff Acknowledgments

In addition to the contact names above, Andrew Huddleston, Assistant Director; Kay Kuhlman, Assistant Director; Bob Homan, Analyst-in-Charge; Melissa Bodeau; John de Ferrari; Camilo Flores; Erica Miles; Josh Ormond; and Sean Standley made significant contributions to this report.

## 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:

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