

# FTC's Use of Its Authorities to Protect Consumer Privacy and Security

Federal Trade Commission  
2020



## FTC Use of its Authorities to Protect Consumer Privacy and Security

---

This report responds to Senate Appropriations Committee Report 116-111 accompanying the Financial Services and General Government Appropriations Bill, 2020, directing the Federal Trade Commission (“Commission” or “FTC”) to report on “the ways it utilizes its current authorities, including Section 5 unfairness authority, to deter unfair and deceptive conduct in consumer privacy and data security matters.”

Since the enactment of the Fair Credit Reporting Act (“FCRA”)<sup>1</sup> in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy. With the development of the internet as a commercial medium in the 1990s, the FTC expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace.

---

Since the enactment of the Fair Credit Reporting Act (“FCRA”) in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy.

---

As you have requested, we will start by outlining our authority under the FTC Act and Section 5 in particular. We will then discuss some of our other work to deter unfair and deceptive conduct in privacy and data security matters. We will conclude by discussing challenges and limitations of this authority.

### I. The FTC Act

---

Section 5 of the FTC Act prohibits deceptive or unfair commercial practices.<sup>2</sup> Under Section 5, the FTC has aggressively pursued privacy and data security cases in myriad areas, including against social media companies, mobile app developers, data brokers, ad tech industry participants, retailers, and companies in the Internet of Things space.

---

<sup>1</sup> 15 U.S.C. § 1681. Among other things, the FCRA prohibits the unauthorized disclosure of sensitive data used for credit, employment, and other decisions.

<sup>2</sup> 15 U.S.C. § 45. As discussed further below, the Commission also enforces specific statutes containing privacy and data security provisions, such as the Gramm-Leach-Bliley Act (“GLB Act”), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§ 6501-6506; the Telemarketing Sales Rule (“TSR”), 16 C.F.R. Part 310, which gives effect to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101 et seq.; the Controlling the Assault of Non-Solicited Pornography and Marketing (“CAN-SPAM”) Act, 15 USC §§ 7701-7713; and the Fair Credit Reporting Act, 15 U.S.C. § 1681.



To date, the Commission has brought more than 70 cases alleging that companies failed to implement reasonable data security safeguards, and more than 80 general privacy cases.

In order to prove a privacy or security allegation under Section 5, we must show that a company’s conduct is “deceptive” or “unfair.” A representation, omission, or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers – that is, it would likely affect the consumer’s conduct or decisions with regard to a product or service.<sup>3</sup> We have challenged deceptive claims about privacy and security that appear in privacy policies, user interfaces, FAQ pages, company websites, and product packaging. We have challenged claims about what information a company collects, how it uses the information, how long it keeps the information, who it shares the information with, the ability of consumers to exercise choices with respect to the information, and the level of security provided for the information.

---

In order to prove a privacy or security allegation under Section 5, we must show that a company’s conduct is “deceptive” or “unfair.”

---

Notably, some deception cases involve omission of material information, the disclosure of which is necessary to prevent the claim, practice, or sale from being misleading. Thus, for example, we have alleged that a company’s statement that it is collecting “browsing information” is deceptive, where it fails to tell the consumer that it also collected contents of people’s shopping carts, information entered onto banking pages, and search information.<sup>4</sup>

A practice is unfair if (1) it causes or is likely to cause substantial injury (2) the injury is not reasonably avoidable by consumers and (3) the injury is not outweighed by benefits to consumers or competition.<sup>5</sup> We have alleged that several privacy-related practices are unfair, including the following:

---

<sup>3</sup> See FTC Policy Statement on Deception (Oct. 23, 1984) (appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 183 (1984)), <https://www.ftc.gov/public-statements/1983/10/ftc-policystatement-deception>.

<sup>4</sup> See FTC Press Release, *Membership Reward Service Upromise Penalized for Violating FTC Order* (Mar. 17, 2017), <https://www.ftc.gov/news-events/press-releases/2017/03/membership-reward-service-upromise-penalized-violating-ftc-order>; FTC Press Release, *Sears Settles FTC Charges Regarding Tracking Software* (June 4, 2009), <https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software>.

<sup>5</sup> 15 U.S.C. § 45(n).

- Failing to reasonably secure personal information, including financial and health information, and contents of communications.<sup>6</sup>
- Engaging in telephone records pretexting, in which information brokers obtain consumers' phone records under false pretenses (e.g., posing as a customer of a telephone carrier) and sell the information to third parties.<sup>7</sup>
- Soliciting “revenge porn,” in which companies solicit intimate pictures and videos of ex-partners, along with their personal information, without their knowledge or consent.<sup>8</sup>
- Developing and marketing “stalkerware,” in which purchasers surreptitiously install monitoring software on their partners' phones without their knowledge or consent. The software often tracks geolocation, app usage, and contents of text messages and other communications.<sup>9</sup>
- Activating webcams surreptitiously in leased computers placed in consumers' homes.<sup>10</sup>
- Selling sensitive data such as Social Security numbers to third parties that did not have a legitimate business need for the information, including known fraudsters.<sup>11</sup>

---

<sup>6</sup> See, e.g., [In the Matter of InfoTrax Systems, L.C.](#), FTC File No. 162 3130, Docket No. C-4696 (2019); [FTC v. Equifax](#), Civ. Action No. 1:19-cv-03297-TWT (N.D. Ga. 2019); [In the Matter of LightYear Dealer Technologies, LLC, d/b/a DealerBUILT](#), FTC File No. 172 3051, Docket No. C-4687 (2019); [In the Matter of James V. Grago, Jr. and d/b/a ClixSense.com](#), FTC File No. 172 3003, Docket No. C-4678 (2019); [United States of America v. Mortgage Solutions FCS, Inc., d/b/a Mount Diablo Lending](#), Civil Action No. 4:20-cv-00110 (N.D. Cal. 2019); [In the Matter of Lenovo, Inc.](#), FTC File No. 152 3134, Docket No. C-4636 (2017); [In the Matter of ASUSTeK Computer Inc.](#), FTC File No. 142 3156, Docket No. C-4587 (2016); [In the Matter of LabMD, Inc.](#), FTC File No: 102 3099; Docket No. C-9357, Civil Action No. 16-16270 (11th Cir. 2015); [In the Matter of Accretive Health, Inc.](#), FTC File No. 122 3077, Docket No. C-4432 (2013); [In the Matter of TRENDnet, Inc.](#), FTC File No. 122 3090, Docket No. C-4426 (2013); [In the Matter of HTC America, Inc.](#), FTC File No. 122 3049, Docket No. C-4406 (2013); [In the Matter of Compete, Inc.](#), FTC File No. 102 3155 (2012); [In the Matter of EPN, Inc., also d/b/a as Checknet, Inc.](#), FTC File No. 112 3143, Docket No. C-4370 (2012); [US v. Direct Lending Source, Inc., Bailey & Associates Advertising, Inc., Virtual Lending Source, LLC](#), FTC File No. 102 3000, Civil Action No. 12-CV-2441-DMS-BLM (S.D. Cal. 2012); [FTC v. Wyndham Worldwide Corp., Wyndham Hotel Group, LLC, Wyndham Hotels & Resorts, LLC, and Wyndham Hotel Management, Inc.](#), Civil Action No. 2:12-cv-01265-SPL (D.N.J. 2012).

<sup>7</sup> See [FTC v. Accusearch, Inc.](#), Case No. 08-8003 (10th Cir. 2009).

<sup>8</sup> See [FTC and State of Nevada v. EMP Media, Inc. \(d/b/a MyEx.com\)](#), Civil Action No. 2:18-cv-00035 (D. Nev. 2018); [In the Matter of Craig Brittain](#), FTC File No. 132 3120 Docket No. C-4564 (2015).

<sup>9</sup> See [In the Matter of Retina-X Studios, LLC](#), FTC File No. 172 3118 (2019).

<sup>10</sup> [In the Matter of DesignerWare, LLC](#), Docket No. C-4390 (F.T.C. Apr. 15, 2013); [In the Matter of Aaron's, Inc.](#), FTC File No. 122 3256 (2013).

<sup>11</sup> [FTC v. Sitemsearch Corp., d/b/a LeapLab; LeapLab, LLC; Leads Company, LLC](#), FTC File No. 142 3192, Case No. 2:14-cv-02750 (D. Ariz. Feb. 18, 2016); [FTC v. Sequoia One, LLC](#), Case No. 2:15-cv-01512-JCM-CWH (D. Nev. Nov. 2, 2016); [FTC v. Blue Global, LLC](#), Case No. 2:17-cv-02117-ESW (D. Ariz. July 5, 2017).



- Collecting and sharing sensitive television-viewing information without notice or consent.<sup>12</sup>
- Where a company does not make a deceptive representation or omission, and we cannot prove the three prongs of unfairness, we cannot bring a Section 5 case.<sup>13</sup>

In terms of remedies under Section 5, our orders in these cases include, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally-obtained consumer information, and/or requirements to improve transparency and choice mechanisms for consumers. The FTC generally cannot seek civil penalties for initial violations of the FTC Act, but if a company violates an FTC order, the FTC can seek civil monetary penalties for the violations, as it did last year when it announced a \$5 billion settlement with Facebook.<sup>14</sup>

The Commission recognizes that achieving effective remedies is a dynamic process that involves continual review of what has been working and what needs further adjustment or strengthening. Thus, from time to time, the Commission has revised standard provisions in orders in order to improve their effectiveness. For example, last year, the Commission worked to strengthen data security orders to require board-level oversight of data security issues where appropriate, set forth more specific requirements (e.g., requirements to encrypt data, segment networks), and improve the accountability of third-party data security assessors.<sup>15</sup>

---

The FTC can seek civil monetary penalties for the violations, as it did last year when it announced a \$5 billion settlement with Facebook.

---



---

<sup>12</sup> [FTC v. Vizio, Inc.](#), 2:17-cv-00758 (D.N.J. 2017).

<sup>13</sup> The FTC continues to examine new and emerging technology areas, such as biometrics, artificial intelligence, ed tech, and voice-activated devices.

<sup>14</sup> See FTC Press Release, *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

<sup>15</sup> The appellate court decision in *LabMD* also was part of the impetus for the Commission to re-evaluate the data security provisions in its orders. In that decision, the court found, *inter alia*, that the requirement to “establish, implement, and maintain a reasonable data security program” was unenforceable because of lack of specificity. *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221, 1237 (11th Cir. 2018). The result in that case underscores the challenges the Commission faces when litigating violations of Section 5 of the FTC Act stemming from data security practices and the need for federal data security legislation.

The FTC Act also authorizes the Commission to promulgate trade regulation rules to address prevalent unfair or deceptive practices, and to seek civil penalties against those who violate them with actual knowledge or with knowledge fairly implied.<sup>16</sup> Section 18 of the FTC Act, 15 U.S.C. § 57a, added by the Magnuson-Moss Warranty—FTC Improvements Act, Pub. L. No. 93-637 (1975), establishes a set of procedures that the FTC must follow in promulgating these rules. These procedures include the following: (1) publication of an advance notice of proposed rulemaking (“ANPR”), an opportunity for public comment on the ANPR, and a determination by the Commission, before issuing a notice of proposed rulemaking, that the acts or practices at issue are “prevalent;” (2) submission of both the ANPR and the NPR to Congressional oversight committees; (3) a mandatory oral hearing, if any person requests one, presided over by an independent hearing officer; (4) preparation of a staff report and recommendations to the Commission on the rulemaking record; (5) submission of the hearing officer’s recommended decision to the Commission; (6) a public comment period; (7) special judicial review provisions that allow parties to apply to the court for leave to make additional oral submissions or written presentations. Even under the best of circumstances, this would be a lengthy process.<sup>17</sup> For a variety of reasons, the Commission has not engaged in this type of rulemaking on privacy and security.

## II. Other Authority

---

In addition to the FTC Act, the FTC has authority to enforce a variety of specific laws in the privacy area, including the Gramm-Leach-Bliley Act (“GLB”), which protects the privacy of financial information; the CAN-SPAM Act, which allows consumers to opt out of receiving commercial email messages; the Children’s Online Privacy Protection Act (“COPPA”); the Fair Credit Reporting Act (“FCRA”), which protects the privacy of consumer report information; the Fair Debt Collection Practices Act, which protects consumers from harassment by debt collectors; and the Telemarketing and Consumer Fraud and Abuse Prevention Act, under which the FTC implemented the Do Not Call registry.<sup>18</sup> The FTC has brought

---

The FTC has brought more than 100 cases against companies for violating the FCRA, and close to 30 COPPA cases.

---

<sup>16</sup> 15 U.S.C. § 57a.

<sup>17</sup> See 15 U.S.C. §§ 57a & § 57b-3; 16 C.F.R. § 1.13.

<sup>18</sup> See Gramm-Leach-Bliley Act (“GLB Act”), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM Act”), 15 U.S.C. §§ 7701-7713; Children’s Online Privacy

more than 100 cases against companies for violating the FCRA, and close to 30 COPPA cases. Since 2003, the FTC has brought 147 cases enforcing Do Not Call provisions against telemarketers, and more than 130 spam and spyware cases. Since 2005, the FTC has brought about 35 cases alleging violations of the GLB Act and its implementing regulations. The Commission has used these authorities to take action against large, well-known companies such as YouTube and Equifax, as well as smaller companies that we allege to have engaged in illegal practices, such as, most recently, a mortgage company that retaliated against consumers by disclosing consumers' credit information on Yelp, in violation of the Fair Credit Reporting Act and other statutes.<sup>19</sup> In contrast to Section 5, many of these statutes allow us to seek civil penalties for first time violations.

In addition to our enforcement efforts on privacy and data security, the Commission seeks to improve agency decision-making through its policy initiatives. Since 2010, we have conducted 45 workshops on privacy issues and issued 29 reports. For example, over the past 18 months, the Commission held four days of hearings that specifically addressed consumer privacy and data security.<sup>20</sup> The Commission also announced its fifth PrivacyCon, which will take place on July 21, 2020, an annual event that explores evolving privacy and data security research.<sup>21</sup> Finally, the Commission is empowered to conduct industry studies related to privacy and data security under Section 6(b) of the FTC Act.<sup>22</sup> Last year, we issued 6(b) orders to several internet service providers to

---

Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506; Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681; Fair Debt Collection Practices Act ("FDCPA"), 15 U.S.C. § 1692; Telemarketing and Consumer Fraud Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108.

<sup>19</sup> See FTC Press Release, *Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law* (Sept. 4, 2019), <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>; FTC Press Release, *Equifax to Pay \$575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related>; FTC Press Release, *Mortgage Broker That Posted Personal Information about Consumers in Response to Negative Yelp Reviews Settles FTC Allegations* (Jan. 7, 2020), <https://www.ftc.gov/news-events/press-releases/2020/01/mortgage-broker-posted-personal-information-about-consumers>.

<sup>20</sup> See FTC Press Release, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21<sup>st</sup> Century* (Oct. 26, 2018), <https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its>.

<sup>21</sup> See FTC Press Release, *FTC Announces PrivacyCon 2020 and Calls for Presentations* (Oct. 11, 2019), <https://www.ftc.gov/news-events/press-releases/2019/10/ftc-announces-privacycon-2020-calls-research-presentations>.

<sup>22</sup> 15 U.S.C. § 46(b).



report on their privacy practices.<sup>23</sup> As we have in the past, we will use the information we learn from this study to better inform our policy and enforcement work.

In all of our privacy and data security work, the FTC's goals have remained constant: to protect consumers' personal information and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace. The attached Appendix provides additional details about how we have used our existing authority. Appendix A (Federal Trade Commission 2019 Privacy and Data Security Update).

### III. Challenges and Limitations

Despite our use of these authorities, we face several limitations and challenges. First, Section 5 does not generally allow the Commission to seek civil penalties for a first-time offense. Relatedly, because our Section 5 authority relies heavily on individual case enforcement and judicial interpretation, adverse

decisions can have an outsized effect on our enforcement ability. For example, recent decisions questioning our ability to obtain injunctive and monetary relief have allowed opposing parties to challenge the agency's pursuit of that relief,<sup>24</sup> presenting further hurdles in obtaining monetary relief for consumers in this area.<sup>25</sup>

Second, while we have Administrative Procedure Act ("APA") rulemaking authority for specific statutes (like COPPA), we do not have APA rulemaking authority generally, which limits how quickly rules can be made. While the Commission possesses Magnuson-Moss rulemaking authority under Section 18 as discussed above, targeted authority to enact

---

Section 5 does not generally allow the Commission to seek civil penalties for a first-time offense.

---

<sup>23</sup> See FTC Press Release, *FTC Seeks to Examine the Privacy Practices of Broadband Providers* (Mar. 26, 2019), <https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers>.

<sup>24</sup> See, e.g., *FTC v. Zurixx, LLC*, 2020 WL 927531 (D. Utah Feb. 26, 2020); *FTC v. Simple Health Plans, LLC*, 2020 WL 570811 (11th Cir. Feb. 5, 2020); *FTC v. Nudge*, 2019 WL 7398678 (D. Utah Dec. 31, 2019); *FTC v. AMG Capital Mgmt., LLC*, 910 F.3d 417 (9th Cir. Dec. 3, 2018), *petition for cert. filed* (U.S. Oct. 18, 2019).

<sup>25</sup> *F.T.C. v. Credit Bureau Center, LLC*, 937 F.3d 764, 767 (7th Cir. 2019) (holding section 13(b) does not authorize restitutionary relief, and overruling *FTC v. Amy Travel Service, Inc.*, 875 F.2d 564 (7th Cir. 1989)); *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221, 1237 (11th Cir. 2018) (holding that FTC order was unenforceable because of lack of specificity); and *Kokesh v. S.E.C.*, 137 S.Ct. 1635, 1639 (2017) (holding disgorgement in the securities-enforcement context is a "penalty" within the meaning of a securities statute similar to Section 5, so disgorgement actions must be commenced within five years of the date the claim accrues).



privacy rules under the APA would better allow us to ensure that the law keeps up with changes in technology. As noted above, Magnuson-Moss rulemaking authority is a more complex process that requires additional procedural hurdles and historically has taken significantly longer than rulemakings that proceed under the APA, rendering it an imperfect tool for the rapidly evolving space of data privacy.<sup>26</sup> See 15 U.S.C. § 57a. Where Congress has given us APA rulemaking authority, we have used it. For example, Congress enacted COPPA in 1998, at a time when children were not using mobile devices or uploading photos on social media sites. In 2012, the Commission used its APA rulemaking authority to expand the parental consent required under COPPA to photos and videos uploaded by children, and to apply the statute to the collection of persistent identifiers, like IP addresses. It also clarified that the collection of geolocation information would trigger COPPA's requirements.

Third, Section 5 excludes non-profits and common carriers from the Commission's authority, even when the acts or practices of these market participants have serious implications for consumer privacy and data security. Indeed, many data breaches over the years have taken place in the non-profit educational sector.

For these reasons, to better equip the Commission to meet its statutory mission to protect consumers, we urge Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers.<sup>27, 28</sup>

---

<sup>26</sup> Specifically, to propose a Mag-Moss rule, the Commission will be required to, among other things, publish an Advance Notice of Proposed Rulemaking with a 30-day public comment period, provide an opportunity for public hearings, publish a staff report, receive and review a presiding officer report on any hearings, and hold a 60-day public comment period on the staff and presiding officer reports. 15 U.S.C. § 57a; 16 C.F.R. § 1.13.

<sup>27</sup> Commissioner Phillips supports congressional efforts to consider consumer data privacy legislation. He believes legislation should be based on harms that Congress agrees warrant a remedy, and that tools like penalties and rulemaking should be calibrated carefully to address those harms. Commissioner Phillips believes Congress should also give appropriate consideration to the trade-offs involved in new regulation, and, with regard to rulemaking, reserve to itself fundamental value judgments appropriately made by the legislature. Finally, Commissioner Phillips believes data security legislation is a critical step Congress should also take to protect consumer privacy.

<sup>28</sup> See also Concurring Statement of Commissioner Rohit Chopra, *Issuance of Federal Trade Commission Report, FTC's Use of Its Authorities to Protect Consumer Privacy and Security* (June 18, 2020), available at <https://www.ftc.gov/public-statements/2020/06/statement-commissioner-rohit-chopra-regarding-report-congress-ftcs-use-its>.

## Appendix: Federal Trade Commission 2019 Privacy and Data Security Update<sup>1</sup>

---

The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Gramm-Leach-Bliley Act, the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. The Commission has used its authority to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models.

### How Does the FTC Protect Consumer Privacy and Promote Data Security?

The FTC uses every tool at its disposal to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take steps to remediate the unlawful behavior. This has included, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and providing robust transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, the Telemarketing Sales Rule, the Fair Debt Collection Practices Act, and the CAN-SPAM Act.

---

The FTC uses every tool at its disposal to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take steps to remediate the unlawful behavior.

---

Using its existing authority, the Commission has brought hundreds of privacy and data security cases to date. To better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested

<sup>1</sup> This document covers the time period from January 2019-December 2019. It will be re-issued on an annual basis.

legislation would expand the agency’s civil penalty authority, provide the agency with targeted rulemaking authority, and extend the agency’s commercial sector jurisdiction to non-profits and common carriers as well.

Beyond enforcement, the FTC’s tools include conducting studies and issuing reports, hosting public workshops, developing educational materials for consumers and businesses, testifying before the U.S. Congress and commenting on legislative and regulatory proposals that affect consumer privacy, and working with international partners on global privacy and accountability issues.

In all of its privacy and data security work, the FTC’s goals have remained constant: to protect consumers’ personal information; and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace.

## ENFORCEMENT




The FTC, building on decades of experience in consumer privacy enforcement, continued in 2019 to conduct investigations and bring cases addressing practices offline, online, and in the mobile environment, as described below. The FTC’s cases generally focus on protecting American consumers, but in some cases also protect foreign consumers from unfair or deceptive practices by businesses subject to the FTC’s jurisdiction.

### General Privacy

The FTC has brought enforcement actions addressing a wide range of privacy issues in a variety of industries, including social media, ad tech, and the mobile app ecosystem. These matters include **more than 130 spam and spyware cases** and **80 general privacy lawsuits**. In 2019, the FTC announced the following privacy cases:

- ▶ On July 24, 2019, the Commission and the U.S. Department of Justice announced a settlement with [Facebook](#). The complaint alleged that Facebook violated the Commission’s 2012 order against the company by misrepresenting the control users had over their personal information, and failing to institute and maintain a

reasonable program to ensure consumers’ privacy. It also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users. The [Facebook order](#) imposed a \$5 billion penalty, as well as a host of modifications to the Commission’s order designed to change Facebook’s overall approach to privacy. The \$5 billion penalty against Facebook is the largest ever imposed on

FTC Settlement with Facebook	
	<b>\$5,000,000,000</b> Unprecedented <b>penalty</b>
	New <b>privacy structure</b> at Facebook
	New tools for FTC to <b>monitor</b> Facebook

any company for violating consumers' privacy. The settlement is currently pending approval by the United States District Court for the District of Columbia.

- ▶ In a related, but separate case, the FTC also filed a law enforcement action against the data analytics company [Cambridge Analytica](#), as well as its former Chief Executive Officer, Alexander Nix, and app developer, Aleksandr Kogan. The FTC's complaint alleged that Cambridge Analytica, Nix, and Kogan used false and deceptive tactics to harvest personal information from millions of Facebook users for voter profiling and targeting. The complaint alleged that app users were falsely told the app would not collect users' names or other identifiable information. Contrary to this claim, the complaint alleged, the app collected users' Facebook User ID, which connects individuals to their Facebook profiles. [Kogan](#) and [Nix](#) agreed to settlements with the FTC that restrict how they conduct any business in the future, and the Commission entered a default judgment against [Cambridge Analytica](#). The Commission's [opinion](#) holds that Cambridge Analytica violated the FTC Act through the deceptive conduct and reaffirms the proposition that, like any other claim, a company's privacy promises are viewed through the lens of established FTC consumer protection principles.

- ▶ The FTC brought its first action against a developer of stalking apps—software that allows purchasers to monitor the mobile devices on which they are installed, without users' knowledge. In its complaint, the FTC alleged, among other things, that [Retina-X](#) sold apps that required circumventing certain security protections implemented by the mobile device operating system or manufacturer, and did so without taking reasonable steps to ensure that the apps would be used only for legitimate and lawful purposes. The [complaint](#) alleged that the company's practices enabled use of its apps for stalking and other illegitimate purposes. The proposed order requires the company and its owner to refrain from selling products or services that monitor devices, without taking steps to ensure that the products or services will be used for legitimate purposes.



- ▶ [Unrollme, Inc.](#), an email management company, settled allegations that it deceived consumers about how it accesses and uses their personal emails. According to the complaint, [Unrollme](#) falsely told consumers that it would not “touch” their personal emails in order to persuade consumers to provide access to their email accounts. In fact, the complaint alleged, Unrollme was sharing the consumers' email receipts—which can include, among other things, the user's name, billing and shipping addresses, and information about products or services purchased by the consumer—with its parent company, Slice Technologies, Inc. According to the complaint, Slice used anonymous purchase information from Unrollme users' e-receipts in the market research analytics products it sells. As part of the [settlement](#) with the Commission, Unrollme is prohibited from misrepresenting the extent to which it collects, uses, stores, or shares

information from consumers. It is also required to notify consumers and delete the data unlawfully collected from consumers, unless it obtains their affirmative, express consent to maintain the e-receipts.

- ▶ In [Effen Ads, LLC \(iCloudWorx\)](#), the FTC obtained stipulated final orders against defendants that promoted a work-from-home program through unsolicited email, or spam, claiming that consumers could make significant income with little effort. The spam emails included misleading “from” lines and links to websites that falsely claimed that various news sources had favorably reviewed the program, and “subject” lines that displayed false celebrity endorsements. The stipulated final orders permanently ban defendants from marketing or selling either work-from-home programs or business opportunities or business coaching products, and permanently enjoined them from violating the CAN-SPAM Act. The orders also impose judgments totaling more than \$12.6 million, and require defendants to pay nearly \$1.5 million in partial satisfaction of the judgments.
- ▶ In [Global Asset Financial Services Group, LLC](#), the FTC shut down a phantom debt brokering and collection scheme. The Commission charged the defendants with purchasing and collecting on counterfeit debts fabricated from misappropriated information about consumers’ identities as well as finances and debts purportedly owed on bogus “autofunded” payday loans. In numerous instances, defendants also disclosed consumers’ purported debts to third parties. The final orders, imposing a combined judgment of more than \$13 million, ban all the defendants from the debt collection business and from misleading consumers about debt. They also prohibit defendants from profiting from customers’ personal information collected as part of the challenged practices, and failing to dispose of such information properly.
- ▶ In [Hylan Asset Management, LLC](#), the FTC and the New York Attorney General’s Office charged two operations—Hylan Asset Management, LLC and its related companies (Hylan) and Worldwide Processing Group, LLC (Worldwide)—as well as their principals with buying, placing for collection, and selling lists of phantom debts, including debts that were fabricated by the defendants or disputed by consumers. The Commission alleged that the defendants obtained consumers’ private financial information and then used it to convince consumers they were legitimate collectors calling about legitimate debts. The FTC also alleged that, in numerous instances, the Worldwide defendants unlawfully communicated with third parties where they already possessed contact information for the consumer. The FTC secured final orders banning the Hylan defendants from the debt collection industry and prohibiting the Worldwide defendants from unlawful debt collection practices. The orders prohibit all defendants from using customers’ personal information and failing to properly dispose of that information.
- ▶ In [ACDI Group](#), the Commission charged the defendants with collecting on a portfolio of counterfeit payday loan debts, which included financial information, such as Social Security and bank account numbers. When the defendants reported to the debt broker who had sold them the portfolio that they had

received consumer complaints regarding the legitimacy of the debts, the broker returned the defendants' money and told them to stop collecting; however, the defendants allegedly continued to do so for at least seven more months. The final order, entered in December 2019, requires the defendants to provide full redress to injured consumers and prohibits the defendants from disclosing, using, or benefitting from previously obtained consumer information that is unverified.




- ▶ In [Grand Teton Professionals LLC](#), the FTC charged defendants with running a credit repair scheme that collected more than \$6.2 million in illegal upfront fees and falsely claimed to repair consumers' credit. Among other things, the Commission alleged that the operation obtained sensitive consumer data, like Social Security numbers and dates of birth, for bogus credit repair services.
- ▶ In [Mission Hills Federal](#), the FTC obtained a temporary restraining order halting a student loan debt relief scheme. The defendants promised student loan assistance and allegedly then used consumer's personal information to effectively assume consumers' identities with their federal loan servicers. According to the FTC's filings, the defendants did this to prevent consumers from learning the defendants were actually pocketing millions of dollars in consumers' student loan payments instead of paying down their loans or providing debt relief.
- ▶ In [Career Education Corporation](#), the FTC obtained stipulated final orders against defendants that used deceptive lead generators to market their schools. The defendants' lead generators used deceptive tactics, such as posing as military recruiting websites, to induce consumers to provide their information online. Those websites promised consumers that the information submitted would not be shared with anyone else, but the lead generators sold that information to the defendants to market their schools. The stipulated final order imposes a \$30 million judgment for consumer redress, and requires defendants to launch a system to review the materials that lead generators use to market their schools, to investigate complaints about lead generators, and to not use or purchase leads obtained deceptively or in violation of the Telemarketing Sales Rule.

## Data Security and Identity Theft

Since 2002, the FTC has brought **more than 70 cases** against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. In 2019, the FTC strengthened its standard orders in data security cases. Each of the cases discussed below resulted in settlements that, among other things, required the companies to implement a comprehensive security program, obtain robust biennial assessments of the program, and submit annual certifications by a senior officer about the company's compliance with the order.

- ▶ The FTC’s complaint against [Equifax](#) alleged that the company failed to secure the massive amount of personal information stored on its network. Among other things, the company allegedly failed to patch well-known software vulnerabilities, failed to segment its database servers, and stored Social Security numbers in unencrypted, plain text. According to the complaint, these failures led to a breach that affected more than 147 million people, and exposed millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud. The [settlement](#), which totals between \$575 million and \$700 million, was part of a global resolution where Equifax settled matters with a consumer class action, the Consumer Financial Protection Bureau, and 50 states and territories.

**The Equifax Breach – A Global Settlement**

	\$575,000,000+ settlement
	Free credit monitoring and identity theft services
	Strong <b>data security</b> requirements

→ Learn more: [ftc.gov/Equifax](https://ftc.gov/Equifax)

Source: Federal Trade Commission | FTC.gov

- ▶ In July, the FTC announced a complaint and settlement against the operator of [ClixSense.com](#), an online rewards website that pays its users to view advertisements, perform online tasks, and complete online surveys. The complaint alleged that the website’s operator, James V. Grago, Jr., deceived consumers by falsely claiming that ClixSense “utilizes the latest security and encryption techniques to ensure the security of your account information.” In fact, ClixSense failed to implement minimal data security measures and stored personal information—including Social Security numbers—in clear text with no encryption, according to the complaint. The FTC alleged that ClixSense’s failures allowed hackers to gain access to the company’s network, resulting in a breach of 6.6 million consumers’ information.
- ▶ The FTC settled charges against [Unixiz, d/b/a i-Dressup.com](#), a dress-up games website, [alleging](#) that the company and its owners stored and transmitted users’ personal information in plain text and failed to perform vulnerability testing of its network, implement an intrusion detection and prevention system, and monitor for potential security incidents. These failures led to a security breach in which a hacker accessed the information of approximately 2.1 million users—including approximately 245,000 users who indicated they were under 13.
- ▶ As discussed above, the FTC alleged that [Retina-X, a company that sold so-called “stalking apps.”](#) and its owner claimed that “Your private information is safe with us.” Despite this claim, the company and its owner failed to adopt and implement reasonable information security policies and procedures.
- ▶ In its complaint against a provider of software to help auto dealers with management of their inventory, personnel, and customers, the FTC alleged that [LightYear Dealer Technologies, LLC, d/b/a DealerBuilt](#) failed to implement readily available and low-cost measures to protect the personal information it collected. These failures led to a data breach in which a hacker gained access to the

unencrypted personal information—such as Social Security numbers and other sensitive data—of about 12.5 million consumers.

- ▶ The FTC settled charges against [InfoTrax Systems](#), a technology company that provides back-end operation services to multi-level marketers. The FTC alleged that a hacker infiltrated InfoTrax’s server, along with websites maintained by the company on behalf of clients, more than 20 times and accessed the personal information of more than a million consumers. According to the complaint, [InfoTrax](#) and its former CEO, Mark Rawlins, failed to use reasonable, low-cost, and readily available security protections to safeguard the personal information they maintained on behalf of their clients.
- ▶ Smart home products manufacturer [D-Link Systems, Inc.](#) agreed to implement a comprehensive software security program in order to settle FTC allegations over misrepresentations that the company took reasonable steps to secure its wireless routers and Internet-connected cameras. The settlement ended FTC litigation against D-Link stemming from a 2017 complaint in which the agency alleged that, despite claims touting device security, vulnerabilities in the company’s routers and Internet-connected cameras left sensitive consumer information, including live video and audio feeds, exposed to third parties and vulnerable to hackers.

## Credit Reporting & Financial Privacy

The [Fair Credit Reporting Act \(FCRA\)](#) sets out requirements for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has

brought **more than 100 cases** against companies for violating the FCRA and has collected **more than \$40 million in civil penalties**. The [Gramm-Leach-Bliley \(GLB\) Act](#)

requires financial institutions to send customers initial and annual privacy

notices and allow them to opt out of sharing their information with unaffiliated third parties. It also requires financial institutions to implement reasonable security policies and procedures. Since 2005, the FTC has brought about 35 cases alleging violations of the GLB Act and its implementing regulations. In 2019, the FTC brought the following cases:

---

The FTC has brought more than 100 cases against companies for violating the FCRA and has collected more than \$40 million in civil penalties.

---

- ▶ In the [Equifax](#) case, discussed above, the FTC alleged that the credit reporting agency violated the GLB Safeguards Rule. Specifically, the complaint alleged that Equifax failed to design and implement safeguards to address foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; regularly test or monitor the effectiveness of the safeguards; and evaluate and adjust its information security program in light of the results of testing and monitoring, and other relevant circumstances.



- ▶ In [Dealerbuilt](#), discussed above, the FTC alleged that the company violated the Safeguards Rule by failing to: develop, implement and maintain a written information security program; identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; assess the sufficiency of any safeguards in place to control those risks; and design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures.

## International Enforcement

The FTC enforces the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System.

The [EU-U.S. Privacy Shield Framework](#) provides a legal mechanism for companies to transfer personal data from the European Union to the United States. This Framework, administered by the U.S. Department of Commerce, helps protect consumers' privacy and security through an agreed set of Privacy Shield Principles. The FTC plays a role in enforcing companies' privacy promises under the Framework as violations of Section 5 of the FTC Act. This year, the FTC participated, alongside the U.S. Department of Commerce and other U.S. government agencies, in the third [Annual Review](#) of the Framework, which became operational in August 2016. Following the review, the European Commission announced its [continued support](#) for the Privacy Shield, pointing to increased FTC enforcement actions as contributing to the effective functioning of the Framework.

The FTC also serves as a privacy enforcement authority in the [Asia-Pacific Economic Cooperation Cross-Border Privacy Rules \(APEC CBPR\) System](#). The APEC CBPR System is a voluntary, enforceable code of conduct designed to enhance the privacy and security of consumers' personal information transferred among the United States and other APEC members. Under the System, participating companies can be certified as compliant with APEC CBPR program requirements that implement APEC's nine data privacy principles.

Carrying out its enforcement role under these international privacy frameworks, the FTC has brought **64 actions—39 under the previous “[U.S.-EU Safe Harbor](#)” program, 4 under APEC CBPR, and 21 under Privacy Shield.**

---

Carrying out its enforcement role under these international privacy frameworks, the FTC has brought 64 actions—39 under the previous “[U.S.-EU Safe Harbor](#)” program, 4 under APEC CBPR, and 21 under Privacy Shield.

---

During the past year, the FTC brought the following 13 cases:

- ▶ In eight separate actions, the FTC charged that [214 Technologies](#), [Click Labs](#), [DCR Workforce](#), [Incentive Services](#), [LotaData](#), [Medable](#), [SecurTest](#), and [Thru](#) falsely claimed participation in Privacy Shield. While the companies initiated Privacy Shield applications with the U.S. Department of Commerce, the companies did not complete the steps necessary to be certified as complying with the Framework. Because they failed to complete certification, they were not certified participants in the Framework, despite representations to the contrary.
- ▶ In separate actions, the FTC charged that [Empiristat](#), [Global Data Vault](#), and [TDARX](#) falsely claimed participation in Privacy Shield. The companies had allowed their certifications to lapse while still claiming participation. Further, the companies allegedly failed to verify annually that statements about their Privacy Shield practices were accurate, and failed to affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the program.
- ▶ As a part of the FTC's action against [Cambridge Analytica](#), described above, the FTC determined that the company falsely claimed to participate in Privacy Shield after allowing its certification to lapse. Among other things, the Final Order prohibits Cambridge Analytica from making misrepresentations about the extent to which it protects the privacy and confidentiality of personal information, as well as its participation in the EU-U.S. Privacy Shield Framework and other similar regulatory or standard-setting organizations.

## Children's Privacy

The [Children's Online Privacy Protection Act of 1998 \("COPPA"\)](#) generally requires websites and apps to obtain verifiable parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought close to 30 COPPA cases and collected hundreds of millions of dollars in civil penalties. During the past year, the Commission took the following actions:

- ▶ The FTC's settlement with [Google and its subsidiary YouTube](#)—brought in conjunction with the New York Attorney General—alleges that the company collected kids' personal data without parental consent, in violation of the COPPA Rule. The complaint alleges that YouTube violated the COPPA Rule by collecting personal information—including in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent. The \$170 million judgment represents the largest civil penalty amount under COPPA.



- ▶ [Musical.ly](#), now known as TikTok, is the operator of a video social networking app that allows users to create short videos of themselves lip-syncing to music and to share those videos with other users. In 2019, the company paid \$5.7 million to settle charges that it violated COPPA by illegally collecting personal information from children. The complaint alleged the app was child-directed, and that many users self-identified as being under 13.
- ▶ The FTC's complaint against [Unixiz, Inc., d/b/a i-Dressup.com](#), discussed above, alleged that the company and its principals violated COPPA by failing to obtain verifiable parental consent before collecting personal information from children under 13. To gain access to all the features on the website, including the social networking features, users had to register as members by submitting a user name, password, birthdate, and email address. If a user indicated he or she was under 13, the registration field asked for a parent's consent. If a parent declined to provide consent, the under-13 users were given a "Safe Mode" membership allowing them to login to access i-Dressup's games and features but not its social features. The FTC alleges, however, that i-Dressup still collected personal information from these children, even if their parents did not provide consent.
- ▶ In the [Retina-X](#) case, discussed above, the FTC alleged that the respondents failed to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

## Do Not Call

In 2003, the FTC amended the [Telemarketing Sales Rule \(TSR\)](#) to create a national [Do Not Call \(DNC\) Registry](#), which now includes more than **235 million active registrations**. Do Not Call provisions prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the DNC Registry, calling

---

The FTC has brought **147 cases enforcing Do Not Call Provisions against telemarketers.**

---

consumers after they have asked not to be called again, and using robocalls to contact consumers to sell goods or services. Since 2003, the FTC has brought **147 cases enforcing Do Not Call provisions against telemarketers**. Through these enforcement actions, the Commission has sought civil penalties, monetary restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains from the 490 companies and 393 individuals involved. The 139 cases concluded thus far have resulted in orders totaling over \$1.7 billion in civil penalties, redress, or disgorgement, and actual collections exceeding \$160 million. During the past year, the Commission initiated actions and settled or obtained judgments as described below:

- ▶ In the [Educare](#) action, the FTC and the Ohio Attorney General obtained temporary restraining orders, preliminary injunctions, and asset freezes against

an enterprise that ran a fraudulent credit card rate reduction scheme, including four individuals and six corporate entities. One defendant is a provider of Voice over Internet Protocol (“VoIP”) services that transmitted the illegal robocalls for the enterprise. This marks the FTC’s first enforcement action against a VoIP provider. In granting the FTC’s preliminary injunction, the court rejected arguments from the defendants challenging the FTC’s jurisdiction over provision of VoIP services. As the litigation continues, all of the corporate defendants are under a receivership.

- ▶ The FTC obtained a \$30 million civil penalty settlement in its case against [Career Education Corporation](#), discussed above, a post-secondary education company that called numbers on the DNC Registry and used deceptively obtained consumer consent.
- ▶ In the [EduTrek](#) case, the FTC brought claims against some of the deceptive lead generators hired by Career Education Corporation. To lure consumers into providing their contact information through online ads, the defendants used misleading seals of several federal government agencies. The complaint alleges that the defendants made calls to consumers who had submitted their contact information on websites that claim to help them apply for jobs, health insurance, unemployment benefits, Medicaid coverage, or other forms of public assistance. Instead of offering consumers what was promised on the websites, the defendants marketed training and education programs. The defendants allegedly violated the TSR by initiating over five million unsolicited outbound telemarketing calls to numbers on the DNC Registry, and by providing substantial assistance to other telemarketers who placed calls to numbers on the DNC Registry. Litigation continues in this matter.
- ▶ The FTC settled claims with [Media Mix 365](#) and its owners, who developed leads for home solar energy companies. Media Mix called millions of phone numbers on the DNC Registry and repeatedly or continuously called consumers with the intent of annoying, abusing, or harassing them. The settlement imposed a \$7.6 million civil penalty judgment, to be suspended if the defendants made timely payment of \$264,000. The order also permanently bans Media Mix and its owners from violating the TSR.
- ▶ In the [Bartoli](#) action, the FTC resolved claims against a robocaller who blasted millions of illegal robocalls to numbers on the DNC Registry, often using spoofed caller ID numbers. In the last six months of 2017 alone, the complaint alleges that Bartoli placed more than 57 million calls to phone numbers on the Registry. Bartoli had been a telemarketer for several companies the FTC had sued in prior cases. Under the final order, Bartoli is permanently banned from calling phone numbers listed on the DNC Registry, sending robocalls, and using deceptive caller ID practices, such as spoofing. The order also imposed a \$2.1 million civil penalty judgment, which has been suspended based on Bartoli’s inability to pay.

- ▶ The FTC's case against [8 Figure Dream Lifestyle](#), Online Entrepreneur Academy, and their owners preliminarily shut down a fraudulent money making scheme that used illegal robocalls to find victims. The defendants made false or unsubstantiated claims about how much consumers could earn through their programs, often falsely claiming that a typical consumer with no prior skills could make \$5,000 to \$10,000 in 10 to 14 days of buying the program. The FTC obtained a court ordered temporary restraining order and preliminary injunction, together with an asset freeze to preserve funds for potential consumer redress. Litigation continues.
- ▶ In [First Choice Horizon](#), the FTC halted a fraudulent credit card interest rate reduction scheme that contacted its victims through illegal robocalls. The defendants targeted seniors and deceptively told consumers that, for a fee, the defendants could lower their interest rates to zero for the life of the debt, thereby saving the consumers thousands of dollars on their credit card debt. The FTC obtained a temporary restraining order and preliminary injunction, including an asset freeze and the appointment of a receiver to operate the corporate defendants. Litigation is ongoing.
- ▶ In [FTC v. Jasjit Gotra](#), the FTC won a preliminary injunction against lead defendant Gotra, banning him from outbound telemarketing while the case proceeds in litigation against him. The FTC also settled claims with defendant Alliance Security. Alliance Security is a home security installation company that, directly and through its authorized telemarketers, called millions of consumers whose numbers were on the DNC Registry. In its settlement, Alliance Security agreed to a complete ban on all telemarketing. Thus far, through five settlements in the case, the FTC has obtained judgments totaling more than \$14 million.

## ADVOCACY

---

When courts, government agencies, or other organizations consider cases or policy decisions that affect consumers or competition, the FTC may provide its expertise and advocate for policies that protect consumers and promote competition. In 2019, the FTC filed the following comments related to privacy issues:

- ▶ The FTC filed a [comment on National Institute of Standards and Technology \(NIST\) proposed privacy framework](#), which attempts to provide guidance to organizations seeking to manage privacy risks. In the comment, staff of the FTC's Bureau of Consumer Protection commended NIST for proposing a voluntary tool aimed at helping organizations start a dialogue about managing privacy risks within their organizations. The comment suggested certain changes to the proposed framework. For example, it called for greater attention to the need to address the risk of privacy breaches at each step of the Draft Privacy Framework; clarification that procedures for managing privacy risks should account for the sensitivity of the information; and a call for companies to review

whether their actual data practices align with consumer expectations and public-facing statements.

- ▶ The FTC testified before Congress numerous times on privacy and data security issues. For example, the Commission called for privacy and data security legislation in testimony before the [House](#) and [Senate](#) Appropriations Committees and the [House Energy and Commerce Committee](#). The FTC also testified on the need for data security legislation before the [Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations](#) and before the [House Oversight and Reform Subcommittee on Economic and Consumer Policy](#).

## RULES

---

Congress has authorized the FTC to issue rules that regulate specific areas of consumer privacy and security. Since 2000, the FTC has promulgated rules in a number of these areas:

- ▶ The Health Breach Notification Rule requires certain web-based businesses to notify consumers when the security of their electronic health information is breached.
- ▶ The Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. In 2018, the FTC announced a regulatory review, in which it sought public comment to determine whether it should update the Rule in light of new developments in the marketplace. The public comment period closed in 2019, and the FTC is evaluating next steps.
- ▶ The COPPA Rule requires websites and apps to get parental consent before collecting personal information from children under 13. In 2019, as part of its ongoing effort to ensure that its rules are keeping up with emerging technologies and business models, the Commission announced that it was seeking comment on the effectiveness of the 2013 amendments to the COPPA Rule and whether additional changes are needed. The public comment period closed later in 2019, and the FTC is evaluating next steps.
 

The COPPA Rule requires websites and apps to get parental consent before collecting personal information from children under 13.
- ▶ The GLB Privacy Rule sets forth when car dealerships must provide customers with initial and annual notices explaining the dealer's privacy policies and practices, and provide a consumer with an opportunity to opt out of disclosures of certain information to nonaffiliated third parties. The GLB Safeguards Rule requires financial institutions over which the FTC has jurisdiction to develop,

implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards. In 2019, the FTC issued a Notice of Proposed Rulemaking seeking comments on both the GLB Privacy and Safeguards Rules. The public comment period closed later in 2019, and the FTC is evaluating next steps.

- ▶ The Telemarketing Sales Rule requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; limits the hours that telemarketers may call consumers; and sets payment restrictions for the sale of certain goods and services. Do Not Call provisions of the Rule prohibit sellers and telemarketers from calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarketing calls from a particular company. The Rule also prohibits robocalls—prerecorded commercial telemarketing calls to consumers—unless the telemarketer has obtained permission in writing from consumers who want to receive such calls.
- ▶ The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Rule is designed to protect consumers from deceptive commercial email and requires companies to have opt-out mechanisms in place. Following a public comment period as part of its systemic review of all current FTC rules and guides, in 2019 the FTC determined that it would confirm the CAN-SPAM Rule without change.
- ▶ The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.
- ▶ The Pre-screen Opt-out Rule under FACTA requires companies that send “prescreened” solicitations of credit or insurance to consumers to provide simple and easy-to-understand notices that explain consumers’ right to opt out of receiving future offers.
- ▶ In June 2019, the FTC finalized the Military Credit Monitoring Rule, which requires nationwide consumer reporting agencies to provide free electronic credit monitoring services for active duty military consumers. The final Rule requires the nationwide consumer reporting agencies to notify active duty military consumers within 48 hours of any material additions or modifications to their credit files. The Rule also requires that when a credit reporting agency (CRA) notifies an active duty military consumer about a material change to their credit file, the CRA must also provide that consumer with free access to that file. Further, the Rule contains restrictions on secondary uses and disclosures of information collected from an active duty military consumer requesting the credit monitoring service, and also bans marketing during the enrollment process until after an active duty military consumer has been enrolled in the free credit monitoring service.

## WORKSHOPS

Beginning in 1996, the FTC has hosted **more than 75** workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2019, the FTC hosted the following privacy events:

- ▶ In April, as part of the agency's Hearings on Competition and Consumer Protection in the 21st Century, the Commission hosted a hearing on the Commission's authority to deter unfair and deceptive conduct in privacy matters. The FTC's Approach to Consumer Privacy explored topics, such as: the risks and benefits to consumers of information collection, sharing, aggregation, and use; the use of "big data" in automated decisionmaking; how firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data; and what is the best way to provide consumers with the right balance of information with respect to privacy protections.

- ▶ In June, the Commission hosted its fourth annual PrivacyCon, a conference to examine cutting-edge research and trends in protecting consumer privacy and security. The event brought together leading stakeholders, including researchers, academics, industry representatives, federal policymakers, and consumer advocates. PrivacyCon 2019 explored the privacy and security implications of emerging technologies, such as the Internet of Things, artificial intelligence, and virtual reality.



- ▶ In October, the Commission hosted a workshop examining whether to update the COPPA Rule in light of evolving business practices in the online children's marketplace, including the increased use of Internet of Things devices, social media, educational technology, and general audience platforms hosting third-party child-directed content.




- ▶ In December, the Commission, along with the Consumer Financial Protection Bureau, hosted a workshop on accuracy in consumer reporting. The workshop brought together stakeholders—including industry representatives, consumer advocates, and regulators—for a wide-ranging public discussion on the many issues that affect the accuracy of consumer reports. Panels focused on both the accuracy of both traditional credit reports and employment and tenant background screening reports, particularly in light of changes to the marketplace since 2012.





## CONSUMER EDUCATION AND BUSINESS GUIDANCE

The Commission has distributed millions of copies of educational materials, many of which are published in both English and Spanish, and generated millions of online pageviews to help consumers and businesses address ongoing threats to security and privacy. The FTC has developed extensive materials providing guidance on a range of topics, such as identity theft, Internet safety for children, mobile privacy, credit reporting, behavioral advertising, Do Not Call, and computer security. Examples of such education and guidance materials developed in 2019 include:

- ▶ **Cybersecurity for Small Business Campaign.** The FTC continued to promote its Cybersecurity for Small Business campaign, created with the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Small Business Administration (SBA). In 2019, the agency released campaign materials in Spanish covering a dozen topics, including cybersecurity basics, understanding the NIST Cybersecurity Framework, and vendor security. Outreach in 2019 included webinars to state Small Business Development Centers, a social media campaign, regional events for National Small Business Week, a ransomware webinar for Texas municipalities, and presentations to local small business groups.
- ▶ **Tax Identity Theft Awareness Week.** As part of Tax Identity Theft Awareness Week, the FTC held webinars to alert consumers, tax professionals, veterans, and small businesses to ways they can minimize their risk of tax identity theft, and recover if it happens. In 2019, the FTC also joined the U.S. Department of Veterans Affairs, AARP Fraud Watch Network, and the Identity Theft Resource Center to discuss tax identity theft and IRS imposter scams.
 
- ▶ **Mobile Device Privacy & Security.** In 2019, the FTC created new online consumer education about Mobile Payment Apps and updated guidance on how to protect your phone and the data on it. The agency also published blogs on SIM card swap scams, as well as how to protect your personal information when upgrading your phone.
- ▶ **Green Lights & Red Flags: FTC Rules of the Road for Business Seminar.** In August, the FTC held a Rules of the Road workshop in Atlanta, covering data security, truth in advertising, antitrust law basics, and other compliance topics. More than 200 business executives, in-house counsel, law firm practitioners, and ad agency personnel attended. The FTC hosted the day-long program in conjunction with the Office of the Georgia Attorney General, the State Bar of Georgia Antitrust Law Section, and the Better Business Bureau Serving Metro Atlanta.
- ▶ **Identity Theft Program.** The FTC updated its military identity theft publication to reflect the new right to

free online credit monitoring for active duty military. In 2019, the FTC also participated in more than 40 identity theft-related outreach events, including:

speaking at several national conferences on cybercrime and older adults; training Capital One attorneys at a Pro Bono Identity Theft Clinic; speaking at Credit Builders Alliance and World Elder Abuse Awareness Week events; and participating in numerous AARP webinars and tele-town halls. In addition, the agency worked with the Social Security Administration (SSA) to address Social Security imposters and set up IdentityTheft.gov/SSA to help people who get these scam calls. The FTC also worked with AARP to create three videos aimed at Asian American Pacific Islander older adults, helping them avoid IRS imposters, robocalls, and Medicare scams.

---

In 2019, the FTC participated in more than 40 identity theft-related outreach events.

---

- ▶ **Consumer Blog.** The FTC's Consumer Blog alerts readers to potential privacy and data security hazards and offers tips to help them protect their information. In 2019, the most-read consumer blog posts addressed how to avoid Social Security Administration imposters and how to file claims related to the Equifax settlement. In 2019, more than 50 consumer blogs addressed privacy issues, including a Parental Advisory on Dating Apps; hot topics, such as how to avoid BitCoin blackmail; and discussions of new rights, like child credit freezes and free online credit monitoring for active duty military.
- ▶ **Business Blog.** The FTC's Business Blog addresses recent enforcement actions, reports, and guidance. In 2019, there were 44 data security and privacy posts published on the Business Blog. Highlights include: guidance for YouTube channel owners on how to determine if their content is directed to children; analysis of landmark settlements like Facebook and Equifax; a series by the Director of the FTC's Bureau of Consumer Protection on small business cybersecurity; and discussion of emerging issues like genetic testing kits, voice cloning, and stalking apps.



## INTERNATIONAL ENGAGEMENT

---

Part of the FTC's privacy and security work is engaging with international partners. The agency works with foreign privacy authorities, international organizations, and global privacy authority networks to develop mutual enforcement cooperation on privacy and data security investigations. The FTC also plays a role in advocating for globally-interoperable privacy protections for consumers around the world.

## Enforcement Cooperation

The FTC cooperates on enforcement matters with its foreign counterparts through informal consultations, memoranda of understanding, complaint sharing, and mechanisms developed pursuant to the U.S. SAFE WEB Act, which authorizes the FTC, in appropriate cases, to share information with foreign law enforcement authorities and to provide them with investigative assistance using the agency's statutory evidence-gathering powers. Significant enforcement cooperation developments in 2019 include:

- ▶ The FTC collaborated with the United Kingdom's Information Commissioner's Office in its actions against Cambridge Analytica and Aleksandr Kogan and Alexander Nix, described above. To facilitate international cooperation in these cases, the FTC relied on key provisions of the U.S. SAFE WEB Act, which allows the FTC to share information with foreign counterparts to combat deceptive and unfair practices.
- ▶ As part of its work on the management committee of the Global Privacy Enforcement Network (GPEN), the FTC helped to organize a series of teleconference calls and an in-person workshop on accountability and enforcement for GPEN participants. During 2019, GPEN grew to include 69 privacy authorities from 50 countries, with more than 450 staff from participating agencies registered on an internal GPEN discussion forum.

## Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data transferred across national borders. It also works to promote global interoperability among privacy regimes and better accountability from businesses involved in data transfers.

During the past year, in addition to participating in the third Annual Review of the EU-U.S. Privacy Shield Framework, the [FTC played an important role](#) in policy deliberations and projects on privacy and data security internationally. For example, the FTC participated in meetings and activities of the APEC Electronic Commerce Steering Group, the International Working Group on Data Protection in Telecommunications, and the Organisation for Economic Co-operation and Development (OECD), providing input on issues ranging from children's privacy to health-related privacy to the interoperability of privacy regimes.

The FTC also engaged directly with numerous counterparts on privacy and data security issues. The Commission hosted delegations and engaged in bilateral discussions with officials from Chile, Japan, South Korea, Vietnam, and the United Kingdom; the European Commission; members of the European Parliament; and European data protection authorities.

Additionally the FTC conducted technical cooperation missions on privacy and cross-border data transfer issues in India and Brazil.



**Federal Trade Commission**  
[ftc.gov](https://www.ftc.gov)