
FTC Report to Congress on Privacy and Security

A Report to Congress

September 13, 2021



FEDERAL TRADE COMMISSION

Lina M. Khan, Chair
Noah Joshua Phillips, Commissioner
Rohit Chopra, Commissioner
Rebecca Kelly Slaughter, Commissioner
Christine S. Wilson, Commissioner

Contents

- I. Overview of FTC Authority and Highlights of Recent Efforts1**

- II. Priority Areas for Improving the Effectiveness of Our Efforts to Protect Americans’ Privacy.....3**
 - A. Integrating Competition Concerns..... 4
 - B. Advancing Remedies 4
 - C. Focusing on Digital Platforms 6
 - D. Expanding Understanding of Algorithms 6

- III. Resource-Based Needs7**

- IV. Need for Congressional Action10**

This report responds to the Joint Explanatory Statement accompanying the Consolidated Appropriations Act, 2021, P.L. 116-260, directing the Federal Trade Commission (“Commission” or “FTC”) to “conduct a comprehensive internal assessment measuring the agency’s current efforts related to data privacy and security while separately identifying all resource-based needs of the FTC to improve in these areas. The agreement also urges the FTC to provide a report describing the assessment’s findings to the Committees [on Appropriations of the House and Senate] within 180 days of enactment of this Act.”

The report first provides an overview of the FTC’s authority related to privacy and security, highlighting certain recent efforts in those areas. Second, it discusses priorities for improving the effectiveness of our efforts to protect Americans’ privacy. Third, it identifies areas in which we could use additional resources to further ensure Americans’ privacy is protected. Finally, it discusses the need for Congressional action on the FTC’s authority.

I. Overview of FTC Authority and Highlights of Recent Efforts

In lieu of a general privacy or security law, the Commission’s primary source of legal authority in the privacy and data security space is Section 5 of the FTC Act, which prohibits deceptive or unfair commercial acts or practices.¹ Under Section 5, the FTC has 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. 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.² An act or 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.³ Where a company does not make a deceptive representation or omission, or we cannot prove the three prongs of unfairness, we cannot bring a Section 5 case.

In many cases, when we allege violations of the FTC Act, we seek injunctive relief that can include requirements to delete data and algorithms developed with user data, seek consumer consent, provide notices, implement privacy and data security programs, and obtain outside assessments of

¹ 15 U.S.C. § 45.

² 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-policy-statement-deception>.

³ 15 U.S.C. § 45(n).

privacy and data security programs. We may also seek consumer redress. However, the recent Supreme Court opinion in *AMG Capital Management, LLC v. FTC* (“AMG”)⁴ curtails our ability to seek such redress.

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”), which protects the online privacy of children under 13; 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. In contrast to Section 5, many of these statutes allow us to seek civil penalties for first time violations.⁵ The attached [Appendix](#) reflects our most recent accounting of our efforts to enforce these laws.

Many of our recent efforts have focused on addressing the types of privacy concerns that may be heightened by the pandemic and addressing technologies or types of data that may exacerbate existing racial inequities. For example, Americans are facing a host of challenges as a result of the COVID-19 pandemic. In the last year, much of the FTC’s privacy and data security work has dealt with themes that the pandemic has brought to the forefront, such as increased use of health apps⁶, accuracy of data used for housing, employment, and credit⁷, and videoconferencing and ed tech.⁸ Additionally, a recent host of news stories has emerged about how use of data and technology can exacerbate racial disparities.⁹ Some

⁴ *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (2021). In *AMG* the Supreme Court ruled that Section 13(b) of the FTC Act does not allow the Commission to obtain monetary relief in federal court. As a result, the agency lost its best and most efficient tool for returning money to consumers who suffered losses as a result of deceptive, unfair, or anticompetitive conduct, and we urge Congress to take prompt action to restore this authority.

⁵ See, e.g., 15 U.S.C. § 6822(a) (certain provisions of GLB); 15 U.S.C. § 7706(a) (CAN-SPAM); 15 U.S.C. § 6502(c) (COPPA); 15 U.S.C. § 1681s(a)(2) (FCRA); 15 U.S.C. 1692l(a) (Fair Debt Collection Practices Act); 15 U.S.C. § 6102(c) (Telemarketing and Consumer Fraud and Abuse Prevention Act).

⁶ *In the Matter of Flo Health, Inc.*, FTC File No. 1923133 (2021), <https://www.ftc.gov/enforcement/cases-proceedings/1923133/flo-health-inc>.

⁷ See, e.g., *U.S. v. Appfolio, Inc.*, Civil Action No. 1:20-cv-03563 (D.D.C. 2020), <https://www.ftc.gov/enforcement/cases-proceedings/1923016/appfolio-inc>; *U.S. v. MyLife.com, Inc.*, Civil Action No. 2:20-cv-06692 (C.D. Cal. 2020), <https://www.ftc.gov/enforcement/cases-proceedings/182-3022/mylifecom-inc>.

⁸ See, e.g., *In the Matter of Zoom Video Communications, Inc.*, FTC File No. 1923167, Docket No. C-4731 (2021), <https://www.ftc.gov/enforcement/cases-proceedings/192-3167/zoom-video-communications-inc-matter>; FTC Business Blog, *COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus* (Apr. 9, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schoolsduring-coronavirus>; FTC Consumer Blog, *Remote learning and children’s privacy* (Apr. 9, 2020), <https://www.consumer.ftc.gov/blog/2020/04/remote-learning-and-childrens-privacy>.

⁹ See, e.g., Kashmir Hill, “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match,” N.Y. TIMES (Jan. 6, 2021), <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>; Zak Doffman, “Black Lives

of our recent work has focused on this issue. For example, we have collected research on racial equity issues¹⁰, issued business guidance on artificial intelligence and algorithms¹¹, conducted enforcement related to facial recognition¹² and credit discrimination,¹³ and implemented the FTC’s Every Community Initiative, which examines consumer protection issues and the impact of unlawful privacy practices on distinct groups, including Black Americans, Latinos, Asian Americans, Native Americans, older adults, military service members and veterans, and other groups.¹⁴

II. Priority Areas for Improving the Effectiveness of Our Efforts to Protect Americans’ Privacy

As demonstrated in Section I, the FTC has been working to target its limited resources toward the most egregious and substantial privacy and security abuses and engaging in outreach with stakeholders to both collect research and information to inform our efforts and to convey important guidance to businesses and consumers. Moving forward, we would like to highlight four areas of FTC focus for improving the effectiveness of our efforts to protect Americans’ privacy: integrating competition concerns, advancing remedies, focusing on digital platforms, and expanding on our guidance on and understanding of the consumer protection and competition implications of algorithms.

Matter: U.S. Protesters Tracked By Secretive Phone Location Technology,” FORBES (June 26, 2020), <https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/>; Ziad Obermeyer, Brian Powers, Christine Vogeli, Sendhil Mullainathan, “Dissecting racial bias in an algorithm used to manage the health of populations,” 366 Science 447 (Oct. 25, 2019), <https://science.sciencemag.org/content/366/6464/447>.

¹⁰ See, e.g., *PrivacyCon 2021* (July 27, 2021), <https://www.ftc.gov/news-events/events-calendar/privacycon-2021>; *PrivacyCon 2020* (July 21, 2020) <https://www.ftc.gov/news-events/events-calendar/privacycon-2020>.

¹¹ FTC Business Blog, *Aiming for truth, fairness, and equity in your company’s use of AI* (Apr. 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>; FTC Business Blog, *Using Artificial Intelligence and Algorithms* (Apr. 8, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>.

¹² *In the Matter of Everalbum, Inc.*, FTC File No. 1923172 (2021), <https://www.ftc.gov/enforcement/cases-proceedings/1923172/everalbum-inc-matter>.

¹³ *FTC v. Liberty Chevrolet, Inc.*, Civil Action No. 1:20-cv-03945-PAE (S.D.N.Y. 2020), <https://www.ftc.gov/enforcement/cases-proceedings/162-3238/bronx-honda>.

¹⁴ The Initiative includes staff throughout the Bureau of Consumer Protection and the FTC’s regional offices who use research and input from stakeholders in communities to develop strategies to prevent fraud, inform the agency’s law enforcement program, and expand outreach. The initiative has recently expanded to include Bureau of Competition staff.

A. Integrating Competition Concerns

We will spend more time on the overlap between data privacy and competition. Many of the largest players in digital markets are as powerful as they are because of the breadth of their access to and control over user data. The FTC has a structural advantage over our counterparts in other jurisdictions that focus exclusively on antitrust or on data protection. Our dual missions can and should be complementary, and we need to make sure we are looking with both privacy and competition lenses at problems that arise in digital markets.

For example, violation of consumer protection laws may be enabled by market power, and consumer protection violations, in turn, can have a detrimental effect on competition. Companies may gain market share through deceptive reassurances on privacy. In addition, in consumer protection cases, we need to look to more competition-based remedies. For example, the FTC's recent complaint against Everalbum, Inc., the developer of the photo storage and organization app, Ever, alleged that the company deceived users about how it would apply facial recognition technology to the photos collected from users. The order requires the company to delete any facial recognition models or algorithms it developed with Ever users' photos or videos.¹⁵ This is an important remedy in the privacy context. Companies should not only have to stop their illegal conduct, they should not be allowed to gain a competitive advantage by benefiting from data they collected unlawfully.

B. Advancing Remedies

The Commission seeks to continuously reevaluate whether it is doing all it can to provide relief for consumers and deter unfair or deceptive privacy and security practices. We aim to give consumers specific, individual relief; stop illegal conduct; and further both specific and general deterrence. To that end, we are focusing on expanding at least four types of remedies: (1) providing notice to harmed consumers; (2) obtaining monetary remedies for harmed consumers; (3) obtaining non-monetary remedial relief for consumers; and (4) not allowing companies to benefit from illegally collected data.

First, in our recent orders, we have been more focused on requiring notice to consumers about a company's unlawful practices. For example, the FTC recently brought its first privacy-related health app case against Flo Health, Inc., alleging that, in violation of its promises to users, the company disclosed health data from millions of users of its Flo Period & Ovulation Tracker app to third parties such as Facebook and Google that provided marketing and analytics services to the app. In addition to a number of other requirements, the settlement requires the company to notify affected users about the disclosure of their personal information.¹⁶ This will give those users useful information to help them to decide whether they still wish to use Flo's services in light of its past actions. It also informs whether users

¹⁵ *In the Matter of Everalbum, Inc.*, FTC File No. 1923172 (2021), <https://www.ftc.gov/enforcement/cases-proceedings/1923172/everalbum-inc-matter>.

¹⁶ *In the Matter of Flo Health, Inc.*, FTC File No. 1923133 (2021), <https://www.ftc.gov/enforcement/cases-proceedings/1923133/flo-health-inc>. In conjunction with the settlement, the FTC also issued guidance to consumers about health apps, with tips for consumers on how to select and use these types of apps while reducing privacy risks. See https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/flo_health_app_infographic_11022020_en_508.pdf.

would recommend the service to others. Finally, notice accords users the dignity of knowing what happened. There is a fundamental equity issue too: many people will not hear about the FTC’s action against a company they deal with unless the company tells them, and those affected by a company’s unlawful activities have a right to know about those actions.

Second, the Commission has looked for ways to get money back to harmed consumers from unfair or deceptive privacy and security practices. For example, our recent settlement with Vivint Smart Home, Inc., includes a \$5 million redress fund for consumers who did not sign up for Vivint’s services but were contacted by debt collectors or found Vivint accounts improperly listed on their credit reports.¹⁷ In other cases, we have supplemented our own authority by partnering with other agencies to get money back to consumers, such as the 2019 Equifax settlement where we worked with the Consumer Financial Protection Bureau (“CFPB”) and 50 U.S. states and territories.¹⁸ In light of the *AMG* decision curtailing our redress authority under Section 13(b), discussed above, it will be especially important that we continue these partnerships.¹⁹

Third, we need to expand non-monetary remedial relief for harmed consumers. In the recent case against Vivint, the FTC alleged that in some instances consumers’ credit information was used by Vivint sales representatives without their knowledge or consent to qualify another individual for financing for Vivint’s products and services. According to the complaint, if customers qualified using these tactics later defaulted on their loans, Vivint referred the innocent third party to its debt buyer, potentially harming that consumer’s credit and subjecting them to debt collectors. To help remediate this harm, the order requires that Vivint establish a customer service task force to verify that accounts belong to the right customer before referring any account to a debt collector, and must assist consumers who were improperly referred to debt collectors.²⁰ This type of relief is important in future cases.

¹⁷ *U.S. v. Vivint Smart Home, Inc.*, Civil Action No. 2:21-cv-00267-TS (D. Utah 2021), <https://www.ftc.gov/enforcement/cases-proceedings/192-3060/vivint-smart-home-inc>.

¹⁸ 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>.

¹⁹ Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), has been the agency’s primary and most effective way of returning to consumers money that was unlawfully taken from them. Thus, the Supreme Court’s recent decision in *AMG Capital Management LLC v. FTC* that 13(b) does not grant the Commission authority to obtain equitable monetary relief deprived the FTC of the strongest tool we had to help consumers when they need it most. The agency’s ability to use Section 13(b) to enjoin illegal activity is also threatened by a recent court decision ruling that the agency cannot bring enforcement actions under Section 13(b) unless a violation is either ongoing or “impending” at the time the suit is filed. *See FTC v. Shire ViroPharma Inc.*, 917 F.3d 147 (3d Cir. 2019). Accordingly, we urge Congress to take quick action to amend Section 13(b) to make clear that the Commission can bring actions in federal court under Section 13(b) even if conduct is no longer ongoing or impending when the suit is filed and can obtain monetary relief, including restitution and disgorgement, if successful.

²⁰ *U.S. v. Vivint Smart Home, Inc.*, Civil Action No. 2:21-cv-00267-TS (D. Utah 2021), <https://www.ftc.gov/enforcement/cases-proceedings/192-3060/vivint-smart-home-inc>.

Finally, we have expanded our efforts to deprive companies of their ability to benefit from illegally-obtained data. These includes remedies requiring deletion of algorithms, such as in the Everalbum case discussed above.

In addition to undertaking these internal efforts, we call on researchers, market experts, and others to advise us on incentives and disincentives that our orders can help create in the marketplace. We will consider making this a topic for a future PrivacyCon conference, where we solicit research papers in areas of interest.

C. Focusing on Digital Platforms

We intend to continue and increase our focus on the data practices of dominant digital platforms. This will allow us to focus most of our limited resources on the most egregious practices and cases against major players in the marketplace in order to have a broader impact.

Part of this work includes a focus on order enforcement. We already have many large companies under order for privacy and/or data security violations, such as Facebook, Google, Twitter, Microsoft, and Uber. If a respondent violates a final administrative order, it may be liable for civil penalties of up to \$43,792 per violation. The Commission's goal must be for our orders to have maximum credibility, disincentivize violative conduct, and improve practices across the market over time. In order to effectuate that goal, the Commission will shift resources to order compliance and enforcement, especially against the largest respondents. We will conduct additional compliance reviews and pursue order modifications and enforcement actions as necessary.

D. Expanding Understanding of Algorithms

We intend to continue our work to deepen our understanding of the consumer protection and competition risks associated with algorithms and to expand upon the guidance that we have provided to businesses on using algorithms and AI truthfully, fairly, and equitably.

For example, every year, the FTC holds PrivacyCon, a conference in which researchers present cutting-edge work on privacy, data security, and artificial intelligence, which helps inform the FTC's policy and enforcement work. PrivacyCon 2020 featured a panel on *Bias in Algorithms* where researchers presented a study demonstrating that an algorithm used with good intentions – to target medical interventions to the sickest patients – ended up funneling resources to a healthier, white population, to the detriment of sicker, black patients.²¹ PrivacyCon 2021 included a panel where panelists discussed research on auditing machine learning algorithms for bias, which was followed by a

²¹ Ziad Obermeyer, Brian Powers, Christine Vogeli, Sendhil Mullainathan, "Dissecting racial bias in an algorithm used to manage the health of populations," 366 Science 447 (Oct. 25, 2019), <https://science.sciencemag.org/content/366/6464/447>.

presentation about a researcher’s algorithmic bias playbook designed to help organizations determine whether they are using biased algorithms and if so, how to mitigate that bias.²²

FTC staff has published a recommendation that companies test their algorithms, both at the outset and periodically thereafter, to make sure it doesn’t create a disparate impact on a protected class.²³ The FTC Act prohibits unfair or deceptive practices. That would include the sale or use of racially biased algorithms. For example, if the developer of an algorithm promises that its product will provide unbiased results, but in fact it does not, that could be a deceptive practice. If a company’s use of a biased algorithm discriminated against consumers, causing them substantial injury that is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition – the FTC could challenge the use of that model as unfair.

III. Resource-Based Needs

Despite the relatively small number of employees, we aim to use our existing resources effectively and efficiently. However, additional resources would allow us to do much more, even within the limits of our current authority, to protect Americans’ privacy. Other, much smaller, countries have much larger numbers of full time employees working on these issues. The FTC’s Division of Privacy and Identity Protection has approximately 40-45 employees. However, the U.K. Information Commissioner’s office has about 768 employees,²⁴ and the Irish Data Protection Commissioner has about 150 employees.²⁵ Although these entities have different mandates,²⁶ as the federal entity primarily responsible for protecting Americans’ privacy and data security, the FTC should have many more employees and access to additional outside resources (such as experts and technologists) without raiding staff working on other critical issues. At the very least, we would need 100 new FTEs to accomplish the goals discussed below.

²² *PrivacyCon 2021* (July 27, 2021), <https://www.ftc.gov/news-events/events-calendar/privacycon-2021>.

²³ FTC Business Blog, *Aiming for truth, fairness, and equity in your company’s use of AI* (Apr. 19, 2021), <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>; FTC Business Blog, *Using Artificial Intelligence and Algorithms* (Apr. 8, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms>.

²⁴ U.K. Information Commissioner’s Annual Report and Financial Statements 2019-20, <https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf>, at 103 (“As at 31 March 2020 the ICO had 768 permanent staff (720.3 full time equivalents)”).

²⁵ Irish Data Protection Commissioner Press Release, *Data Protection Commission statement on funding in 2021 Budget* (Oct. 13, 2020), [https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget#:~:text=The%20Data%20Protection%20Commission%20\(DPC,that%20was%20allocated%20for%202020](https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-funding-2021-budget#:~:text=The%20Data%20Protection%20Commission%20(DPC,that%20was%20allocated%20for%202020) (“Increases in the funding allocated to the DPC in recent years have facilitated the significant expansion of the DPC’s staffing, with an emphasis on strengthening the regulator’s skills-base in the areas of legal, technology, investigations and communications bringing staffing levels to 150 at present”).

²⁶ For example, these entities have responsibilities to supervise the public sector’s collection and use of personal data.

If the FTC were able to obtain increased funding to support additional FTEs,²⁷ we could increase the impact of our privacy and data security work in the following ways:

Expand our Capability to Holistically Address Privacy Abuses. One important way to protect consumer privacy is to closely examine the consolidation and conduct of big tech companies, who can use their monopoly power to engage in unfettered collection and use of consumer data. Our ability to effectively protect consumer privacy depends on the agency being able to tackle these issues on a structural level. This requires a significant infusion of additional FTEs on both the consumer protection and competition side.

Developing and Strengthening Our Tools. Given the serious harms stemming from surveillance practices and the absence of federal legislation, the Commission should deploy all of its tools to protect Americans' privacy. For example, Section 18 of the FTC Act 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. In addition, Section 5 of the FTC Act allows the Commission to promulgate rules to prohibit unfair methods of competition. The Commission can also refine and strengthen its existing toolkit, including the COPPA Rule, the Health Breach Notification Rule, the Red Flags Rule, and the GLB Safeguards Rule.²⁸

Devote Additional Resources to Crucial Areas of Investigation. With additional resources, the FTC would be able to devote additional staff to privacy and security investigations. This would allow us to take on expensive litigation against the largest companies who may be violating the law without forgoing all other enforcement. Priority areas of focus for the Commission, all of which are resource intensive, include:

- The consumer protection and competition implications of business models that depend on expansive and potentially illegal data collection to fuel targeted advertising and user engagement;
- The data practices of dominant digital platforms, which because of their scope and size, may present interrelated privacy and competition concerns;
- Acquisitions that allow dominant digital platforms to collect and control ever expanding data from consumers or block the development of more secure data protection policies;
- Exclusionary or predatory conduct by dominant digital platforms to defend their data troves, resulting in lower levels of privacy and data protections and more intrusive ads;
- Platforms and other online services that are potentially violating COPPA, an area of particular importance given that many children may be increasingly relying on online services for both educational, entertainment, and social purposes during the pandemic;

²⁷ In addition to funding for the FTEs, we would also need funding for the infrastructure to support them, such as space, technology, and equipment.

²⁸ The FTC is currently reviewing a number of privacy and security related rules including the COPPA Rule, the Health Breach Notification Rule, and the Red Flags Rule. The Commission has also issued Notices of Proposed Rulemaking proposing to amend the GLB Privacy and Safeguards Rules following the regulatory review of both Rules. Rule reviews and the rulemaking process are resource intensive.

- Dark patterns, through which companies manipulate user behavior, such as by presenting choices in confusing ways or nudging users toward more data sharing;
- Overlap of privacy, security, and safety concerns, ranging from security concerns created by connected cars and health devices to safety concerns raised by stalking apps and pornography platforms;
- The collection, use, and disclosure of sensitive data, including location data and health data that falls outside of the Health Insurance Portability and Accountability Act, particularly in light of the fact that the pandemic may lead consumers to increasingly turn to various health apps to manage their conditions; and
- The overlap between racial equity issues and privacy, including the potential for algorithmic discrimination in various artificial intelligence applications, such as those that may be used for credit, healthcare, or facial recognition purposes.

Increase Monitoring of Compliance with Existing Orders. As noted above, the Commission plans to target more of its existing resources to monitor compliance with existing orders and engage in order enforcement. But with well-heeled defendants and an increasing number of privacy and security orders, in order to do this most effectively, we need significantly more resources, including potentially millions of dollars to hire more experts.

Expand Our Analytical Capacity. Chair Khan recently appointed a new Chief Technologist who is working to hire additional technologists. We need significant additional resources to hire individuals with knowledge and expertise regarding business and operational practices for information technology that include product development, supply chain management, mergers and acquisitions, customer service, data privacy and analytics, algorithms, information security, network security, the manufacturing of hardware, software development, computer science, and other related fields as necessary to assess the impact of emerging trends on the FTC’s mission to protect the consumer, maintain competition, and pursue organizational effectiveness.

Importantly, technologists, market analysts, and others could conduct extensive industry studies using our authority under Section 6(b) of the FTC Act. We have previously prepared such studies, most recently of mobile device manufacturers and the data broker industry, and are currently studying Internet Service Providers and social media and video streaming companies. The 6(b) orders that the FTC issued to the social media and video streaming companies require them to provide data on how they collect, use, and present personal information, their advertising and user engagement practices, whether they apply algorithms or data analytics to personal information, and how their practices affect children and teens.²⁹ As concerns mount regarding the impact of tech companies on Americans’ privacy and behavior, this study is timely and important and will provide critical information on the business practices deeply embedded in consumers’ digital lives.

²⁹ FTC Press Release, *FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information* (Dec. 14, 2020), <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services>.

IV. Need for Congressional Action

In addition to more resources, the FTC needs Congress to enact new legislation. First, we urge Congress to clarify Section 13(b) of the FTC Act and shore up the FTC's ability to enjoin illegal conduct and revive its authority return to consumers money they have lost, which will greatly assist our efforts to protect consumers. Second, the Commission continues to urge Congress to enact privacy and data security legislation, enforceable by the FTC. Among other important provisions that such legislation will necessarily entail, we hope that it would expand the agency's civil penalty authority, APA rulemaking authority, and jurisdiction over non-profits and common carriers.

Federal Trade Commission 2020 Privacy and Data Security Update

Federal Trade Commission
2020



Federal Trade Commission 2020 Privacy and Data Security Update¹

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 was established more than a century ago, and throughout its history has endeavored to adapt its enforcement approach to changing market demands, including by developing a privacy and data security program. 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?

In the absence of comprehensive general privacy legislation, the FTC has relied on enforcement actions under the general FTC Act and narrower specific statutes as its principal tool to stop law violations and require companies to take steps to remediate the unlawful behavior. This has included 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 transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. In some instances, the FTC can also seek 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.

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 members of Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested legislation would expand the agency's civil penalty authority, provide the agency with more efficient rulemaking authority, and extend the agency's commercial sector jurisdiction to non-profits and common carriers as well.

¹ This document covers the time period from January 2020–December 2020. It will be re-issued on an annual basis.



Beyond case-by-case enforcement, the FTC also develops, amends, and enforces various rules related to privacy and data security. The FTC's rulemaking authority includes specific authority, for example, to issue rules implementing COPPA using the Administrative Procedures Act, and more general authority to address prevalent unfair or deceptive trade practices using Section 18 of the FTC Act. The Commission'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 consistent: to safeguard consumers' personal information; protect them from illegal practices; and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace.

The FTC also takes seriously its obligations to refine its approach by evaluating the effectiveness of its current enforcement strategy and remedies. The Commission is continually looking for ways to better protect consumers' privacy and personal information and prevent unfair data practices.




ENFORCEMENT

The FTC, building on decades of experience in consumer privacy enforcement, continued in 2020 to conduct investigations and bring cases addressing practices offline, online, and in the mobile environment, which help protect the greatest number of consumers, 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 **approximately 80 general privacy lawsuits** in the last 20 years, which have affected hundreds of millions of consumers. In 2020, the FTC announced the following privacy cases:

- ▶ In April, the United States District Court for the District of Columbia [approved the 2019 settlement](#) between [Facebook](#) and the Commission and the U.S. Department of Justice. More than 100 million consumers use Facebook every day to share personal information. The complaint alleged that

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

Facebook violated the Commission's 2012 order against the company by misrepresenting the control users had over their personal information, which tens of millions of users relied upon, 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 any company for violating consumers' privacy.

- ▶ In November, [Zoom](#), which saw its user base grow from 10 million to 300 million during the COVID-19 pandemic, agreed to settle FTC allegations that, since at least 2016, the company misled users by claiming that it offered "end-to-end, 256-bit encryption" to secure users' communications, when, in fact, it provided a lower level of security. According to the FTC's [complaint](#), Zoom also misled some users who wanted to store recorded meetings on the company's cloud storage by falsely claiming that those meetings were encrypted immediately after the meeting ended. Instead, some recordings allegedly were stored unencrypted for up to 60 days on Zoom's servers before being transferred to its secure cloud storage. Finally, Zoom secretly installed software, called a ZoomOpener web server, as part of a manual update for its Mac desktop application in July 2018. The ZoomOpener web server allowed Zoom to automatically launch and join a user to a meeting by bypassing an Apple Safari browser safeguard that protected users from a common type of malware. Without the ZoomOpener web server, the Safari browser would have provided users with a warning box, prior to launching the Zoom app, which asked users if they wanted to launch the app. The software remained on users' computers even after they deleted the Zoom app, and would automatically reinstall the Zoom app—without any user action—in certain circumstances. The [complaint](#) alleges that Zoom's deployment of the ZoomOpener, without adequate notice or user consent, was unfair and deceptive in violation of the FTC Act. Under the proposed [settlement](#), Zoom is prohibited from making misrepresentations about its privacy and security practices. The company must also implement a comprehensive information security program that requires Zoom to implement specific measures aimed at addressing the problems identified in the complaint. The company must obtain biennial assessments of its security program by an independent third party, which the FTC has authority to approve, and notify the Commission if it experiences a data breach.

Data Security and Identity Theft

Since 2002, the FTC has brought **80 cases** against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. In 2020, the FTC continued to apply its strengthened orders in data security cases in order to provide protection for consumers and accountability for businesses. Each of the cases discussed below resulted in settlements that, among other things, required

the company 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.

- ▶ [Tapplock](#) follows a long line of FTC cases related to the Internet of Things and is the first case to allege both data security and physical security vulnerabilities in an Internet-connected device. [Tapplock](#) settled FTC allegations that it deceived consumers by falsely claiming that its Internet-connected smart locks were designed to be “unbreakable” and that it took reasonable steps to secure the data it collected from users. According to the FTC’s [complaint](#), a vulnerability on Tapplock’s API allowed researchers to bypass account authentication and gain full access to all information in Tapplock users’ accounts, including usernames, email addresses, profile photos, location history and precise geolocation of the smart lock. Another vulnerability let researchers lock and unlock any nearby Tapplock smart lock. The [settlement](#) bans Tapplock from making deceptive statements about security of a device or privacy of personal information. It also requires Tapplock to implement a comprehensive security program, including employee training. Finally, the company must get biennial third-party assessments and must certify compliance annually.

- ▶ In its settlement with [SkyMed International, Inc.](#), a company that sells air evacuation plans and other travel emergency services, the FTC [alleged](#) SkyMed failed to employ reasonable measures to secure the personal information it collected from people who had signed up for its emergency travel membership plan, and, as a result, the company left unsecured a cloud database containing approximately 130,000 membership records. The FTC also alleged that SkyMed misrepresented to consumers that it had investigated the data exposure and concluded that no medical data had been exposed, and that the database had not been improperly accessed when, in fact, SkyMed had not investigated the incident and instead merely deleted the database. The complaint also alleged SkyMed deceived consumers by displaying for nearly five years a “HIPAA Compliance” seal on every page of its website, which gave the impression that its privacy policies had been reviewed and met the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA). In fact, no government agency or other third party had reviewed SkyMed’s information practices for compliance with HIPAA. Under the [settlement](#), SkyMed is prohibited from misrepresenting how it secures personal data, the circumstances of and response to a data breach, and whether the company has been endorsed by or participates in any government-sponsored privacy or security program. The company also will be required to send a notice to affected consumers detailing what data was exposed in the security incident. Finally, SkyMed must put in place a comprehensive information security program and obtain biennial assessments of its information security program by a third party, which the FTC has authority to approve. The [settlement](#) also requires a senior SkyMed executive to certify annually that the company is complying with the requirements of the settlement.



- ▶ In the case of [Ascension Data & Analytics, LLC](#), a mortgage industry data analytics company, Ascension hired a vendor to perform text recognition scanning on mortgage documents. The vendor, OpticsML, stored the contents of the documents in two misconfigured cloud storage locations, without any protections to block unauthorized access. As a result, the sensitive personal information of more than 60,000 consumers was left exposed on the internet for a year. In its [complaint](#), the FTC alleged that Ascension violated the Gramm-Leach-Bliley Act's Safeguards Rule, which requires financial institutions to develop, implement, and maintain a comprehensive information security program. As part of that program, financial institutions must oversee their third-party vendors, by ensuring they are capable of implementing and maintaining appropriate safeguards for customer information, and requiring them to do so by contract. They must also identify reasonably foreseeable risks to customer information and assess the sufficiency of any safeguards in place to control those risks. The FTC alleged that, with respect to its vendors such as OpticsML, Ascension failed to do both. As part of a proposed [settlement](#) resolving FTC allegations, Ascension will be required to implement a comprehensive data security program with audits, executive certification, and reporting of future data breaches.

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 \$65 million in civil penalties**. These cases have helped insure that consumer reporting agencies follow reasonable procedures to assure the maximum possible accuracy of consumer report information, so consumers can obtain credit, insurance, employment, and housing. 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, in order to protect the sensitive personal information consumers provide to them. Since 2005, the FTC has brought about **35 cases** alleging violations of the GLB Act and its implementing regulations, which have affected the data security of hundreds of millions of consumers. The [Fair Debt Collection Practices Act \(FDCPA\)](#) covers third-party debt collectors that collect on consumer debt. The FDCPA addresses abusive, deceptive, and unfair debt collection practices, prohibits certain collection tactics, and imposes certain affirmative statutory obligations on collectors. In 2020, the FTC brought the following credit reporting and financial privacy cases:

- ▶ Mortgage Solutions FCS, doing business as [Mount Diablo Lending](#), and its sole owner, Ramon Walker, agreed to pay \$120,000 to settle FTC allegations that they violated the FCRA and other laws by revealing personal information about consumers in response to negative reviews posted on the review website Yelp. In a [complaint](#) filed by the Department of Justice on behalf of the Commission, the FTC alleged that Mount Diablo Lending and Walker responded to consumers



who posted negative reviews on Yelp by in numerous instances revealing their credit histories, debt-to-income ratios, taxes, health, sources of income, family relationships, and other personal information. Several responses also revealed reviewers' first and last names, according to the complaint. The FTC also alleged that the defendants violated the FTC Act and the Gramm-Leach-Bliley Act, including by failing to implement an information security program until September 2017 and by not subsequently testing the program. In addition to paying the FCRA penalty, the defendants are prohibited from misrepresenting their privacy and data security practices, misusing credit reports, and improperly disclosing personal information to third parties. Mount Diablo must also implement a comprehensive data security program designed to protect the personal information it collects and obtain third-party assessments of its information security program every two years. The company must designate a senior corporate manager responsible for overseeing the information security program to certify compliance with the order every year.

- ▶ Section 609(e) of the FCRA requires companies to provide victims of identity theft with application and business transaction records about fraudulent transactions made in their names within 30 days. In its first use of its Section 609(e) authority, the Commission brought a case against [Kohl's Department Stores, Inc.](#) As part of the [settlement](#), Kohl's agreed to pay a civil penalty of \$220,000 to settle allegations that the retailer violated the FCRA by refusing to provide complete records of transactions to numerous consumers whose personal information was used by identity thieves. In addition, Kohl's is required to provide identity theft victims with access to business transaction records related to the theft within 30 days. The company also must post a notice on its website informing identity theft victims about how to obtain records related to identify theft, and certify that it has reached out to victims who were unlawfully denied access to such records in the past.
- ▶ In July, the Department of Justice on behalf of the Commission sued a background check company, [MyLife.com, Inc.](#), and its CEO Jeffrey Tinsley, over allegations that they violated Section 5 of the FTC Act, the FCRA, the Restore Online Shoppers' Confidence Act (ROSCA), and the Telemarketing Sales Rule (TSR). The [complaint](#) alleges that MyLife deceived consumers with "teaser background reports" that often falsely claimed to include information about arrest, criminal, and sex offender records, and also engaged in misleading billing and marketing practices. The complaint also alleges that MyLife is a consumer reporting agency, which assembles and sells millions of consumer reports to American consumers each year, and failed to comply with various requirements set forth by the FCRA. The court denied MyLife's motion to dismiss, and the case is pending in the Central District of California.
- ▶ [AppFolio, Inc.](#), a company that provides background reports about consumers to thousands of property management companies, recently settled allegations that it had failed to ensure maximum possible accuracy of consumer reports, as required by the FCRA. In a [complaint](#) filed by the Department of Justice on behalf



of the Commission, the FTC alleged that AppFolio failed to ensure that criminal and eviction records it received from a third party vendor were accurate before including such information in its tenant screening reports. In addition, the FTC alleged that AppFolio also violated the FCRA by including eviction or non-conviction criminal records more than seven years old in its reports. In multiple instances, the alleged violations may have led to the denial of housing or other opportunities for consumers. As part of the [order](#), AppFolio will pay a \$4.25 million monetary penalty. In addition, the [order](#) prohibits AppFolio from providing non-conviction criminal or eviction records older than seven years and requires the company to maintain reasonable procedures to ensure the maximum possible accuracy of information included in its background reports.

- ▶ In [National Landmark Logistics](#), the FTC secured a temporary restraining order in July 2020 to immediately halt defendants' illegal debt collection practices in violation of the Fair Debt Collection Practices Act (FDCPA). The FTC [alleges](#) that National Landmark Logistics, four related companies, and three individuals took in revenue of at least \$13.7 million through an illegal debt collection scheme, which included pressuring consumers to pay debts they did not actually owe or that the defendants had no right to collect. The defendants typically used robocalls to leave deceptive messages that people were subject to an audit or proceeding or would be served with papers at home or at work. When consumers returned the call to find out more, the FTC says the defendants falsely claimed to be from a mediation or law firm, and that the person was delinquent on a debt. In many instances, collectors threatened consumers with legal action unless they made an immediate credit or debit card payment. To make the pitch seem more believable, collectors often had (or claimed to have) personal information about the supposed debtor, such as their Social Security number, credit card or bank account numbers, or family members' contact information. At the FTC's request, the court granted a [temporary restraining order](#) that provided for the freezing of defendants' assets, the appointment of a temporary receiver, and immediate access to business premises and records.

This case—and the two cases that follow—was brought as part of the Operation Corrupt Collector law enforcement sweep. This initiative, spearheaded by the Commission, was a coast-to-coast law enforcement crackdown, involving cross-coordination with three other federal agencies and partners from 16 states. The sweep encompasses more than 50 actions, targeting some of the worst-of-the-worst debt collection tactics, including phantom debt collection which occurs when companies gain access to consumers' personal information and use it to contact them and pressure them into paying debts they do not owe. As the chief federal agency on privacy and data security, the FTC is focused on protecting consumers from the financial harm that occurs when bad actors mishandle personal information.

- ▶ In [Absolute Financial Services, LLC](#), a companion case to National Landmark Logistics, LLC, the FTC obtained another temporary restraining order. The [complaint](#) charges that Absolute Financial Services, two related companies, and



two individuals collected more than \$6.9 million from consumers, using National Landmark Logistics to place deceptive robocalls on their behalf. The calls claimed that people would be served with important papers or would face legal action or audits if they did not respond. The FTC alleges that once people called back, the defendants' collectors falsely claimed to be representatives of law firms or mediation companies. According to the complaint, the collectors told consumers that they owed on a credit card or other debt and often threatened them with arrest if they did not immediately pay the debt. Using data from National Landmark Logistics, the Absolute Financial Services collectors included pieces of consumers' personal information in an attempt to add an aura of truth to the false statements they made about purported debts. As with National Landmark Services, the court granted the FTC's motion for a [temporary restraining order](#) that froze the defendants' assets, appointed a receiver, and allowed for immediate access to business premises and records.

- ▶ In [Critical Resolution Mediation](#), the FTC obtained a federal court order to shut down an Atlanta-based debt collection operation. The FTC's [complaint](#) alleged that defendants' agents threatened consumers with arrest and imprisonment and tried to collect debts that consumers did not actually owe. According to the FTC, the collectors regularly posed as law enforcement officers, attorneys, mediators, or process servers when calling consumers, lending credence to their threats about supposed unpaid debts. In many cases, the defendants were attempting to collect phantom debts. According to the complaint, the company's collectors threatened not only to arrest and jail consumers who refused to pay immediately, but also to garnish consumers' wages, revoke their drivers' licenses, or lower their credit scores. In addition, the collectors allegedly contacted consumers at their workplaces or notified their families about the supposed debt, shared consumers' personal information, and threatened serious legal consequences. The collectors allegedly used profane language with consumers who refused to pay or asserted their right to review information about the purported debts. The defendants also refused to provide information about the alleged debts as required under the FDCPA. In November 2020, the court entered a stipulated preliminary injunction against all defendants, which maintained the relief secured by the September temporary restraining order, including the freezing of defendants' assets and appointment of a temporary receiver.
- ▶ In [Midwest Recovery Systems](#), the Commission also took action against a debt collection company and its owners that allegedly placed bogus or highly questionable debts onto consumers' credit reports to coerce them to pay the debts, a practice known as "debt parking." Consumers often did not discover these purported debts until they threatened to interfere with important, time-sensitive transactions, such as the purchase of a house or car or an application for employment. The FTC's [complaint](#) alleges that Midwest Recovery Systems received thousands of complaints each month about the purported debts from consumers, with the company itself finding that between 80 and 97 percent of the debts it investigated were inaccurate or not valid. In addition to phantom payday lending debts, the complaint notes that the company parked significant quantities

of medical debt, which is often a source of confusion and uncertainty for consumers because of the complex, opaque system of insurance coverage and cost sharing. The FTC's complaint alleges violations of the FDCPA (including the first federal law enforcement count addressing debt parking), the FCRA, and the FCRA's Furnisher Rule. Under a November 2020 [settlement](#), Midwest Recovery Systems and its owners are prohibited from debt parking and required to delete the debts they previously reported to credit reporting agencies. The settlement includes a monetary judgment of \$24.3 million, which is partially suspended based on an inability to pay. Brandon Tumber, one of the individual defendants and a co-owner of the company, will also be required to sell his stake in another debt collection company and provide the proceeds from that sale to the FTC. In addition, the company will be required to surrender all of its remaining assets. This action marks the first federal law enforcement action against unlawful debt parking, and protects consumers dealing with time-sensitive transactions, such as job searches and home loans, from inaccurate or invalid debts appearing on their credit reports without notice.

International Enforcement

For more than two decades, the FTC has used its enforcement powers to ensure strong privacy protections for consumer data subject to international data transfer mechanisms, such as the EU-U.S. Privacy Shield Framework (and its predecessor program, the U.S.-EU Safe Harbor Framework), the Swiss-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System (APEC CBPRs). On July 16, 2020, the European Court of Justice issued a judgment declaring invalid under EU law the European Commission's Privacy Shield Adequacy Decision of July 12, 2016, and in so doing found the EU-U.S. Privacy Shield Framework inadequate under EU law. On September 8, 2020, the Swiss Federal Data Protection and Information Commissioner issued a position statement adopting the European Court's views. The U.S. Department of Commerce announced, after the EU Court's ruling and the Swiss statement, that these developments do not relieve participants of their obligations under either the EU-U.S. Privacy Shield or the Swiss-U.S. Privacy Shield Framework.

Following the European Court's decision, the FTC stated that companies should continue to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework. The FTC encouraged companies to continue to follow robust privacy principles, such as those underlying the Privacy Shield Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers. Although the European Court of Justice invalidated the Privacy Shield Framework under EU law, that decision does not affect the validity under U.S. law of the FTC's decisions and orders, which typically prohibit companies not just from misrepresenting their compliance with or participation in the Privacy Shield Framework, but also in any other privacy or data security programs sponsored by the government or any self-regulatory or standard-setting organization.



Overall, the FTC has brought **66 actions** to enforce companies' promises under these international privacy programs, 39 under the previous "U.S.-EU Safe Harbor" program, 4 under APEC CBPR, and 23 under Privacy Shield. In 2020, the FTC resolved the following matters arising under the Privacy Shield Framework:

- ▶ The Commission began the year with a number of Privacy Shield cases involving misrepresentations of participation in and compliance with the EU-U.S. Privacy Shield Framework. In January, following a public comment period, the Commission finalized its Privacy Shield settlements with [Click Labs, Inc.](#), [DCR Workforce, Inc.](#), [EmpiriStat](#), [Global Data Vault, LLC](#), [LotaData, Inc.](#), [Incentive Services, Inc.](#), [Medable, Inc.](#), [TDARX, Inc.](#), [Thru](#), and [Trueface.ai](#).
- ▶ In its first Privacy Shield litigation, the Commission sued [RagingWire Data Centers, Inc.](#) administratively over allegations that the company misled consumers about its participation in the EU-U.S. Privacy Shield Framework and failed to adhere to the program's requirements before allowing its certification to lapse. In October, the Commission finalized its [settlement](#) with [NTT Global Data Centers Americas, Inc. \(NTT Global Data Centers\)](#), formerly known as RagingWire Data Centers. Under the settlement, the company, among other things, is prohibited from misrepresenting its compliance with or participation in the Privacy Shield Framework as well as any other privacy or data security program sponsored by the government or any self-regulatory or standard-setting organization. The company also must continue to apply the Privacy Shield requirements or equivalent protections to personal information it collected while participating in the Framework or return or delete the information. Although the European Court of Justice invalidated the Privacy Shield Framework in July 2020, that decision does not affect the validity of the [FTC's decision and order](#) relating to NTT Global Data Centers' misrepresentations about its participation in and compliance with the Framework.
- ▶ The FTC charged that [Ortho-Clinical Diagnostics](#), a provider of medical diagnostic devices, misled consumers about its participation in the Privacy Shield Framework. The FTC alleged that the company claimed to participate in the Privacy Shield Framework and comply with the program's requirements, even though the company had allowed its certification to lapse in 2018. The FTC also alleged Ortho violated the Privacy Shield principles by failing to verify annually that statements about its Privacy Shield practices were accurate. In addition, it also allegedly failed to comply with a Privacy Shield requirement to affirm that the company would continue to apply Privacy Shield protections to personal information collected while participating in the program.
- ▶ The FTC charged that [T&M Protection Resources](#), a background check services provider, misrepresented its participation in and compliance with the Privacy Shield Framework. The company continued to claim participation in the EU-U.S. Privacy Shield after its certification lapsed. In addition, the company failed to verify annually that statements about its Privacy Shield practices were accurate



and failed to affirm that it would continue to apply Privacy Shield protections to personal information collected while participating in the program.

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 age 13. Since 2000, the FTC has brought **34 COPPA cases** and collected **more than \$190 million** in civil penalties. During the past year, the Commission took the following actions:

- ▶ The Commission imposed a \$4 million civil penalty on children's app developer, [HyperBeard](#), for its COPPA violations, which was partially suspended based on inability to pay. In a [complaint](#) filed by the Department of Justice on behalf of the FTC, the Commission alleges that HyperBeard, Inc. violated the COPPA Rule by allowing third-party ad networks to collect personal information in the form of persistent identifiers to track users of the company's child-directed apps, without notifying parents or obtaining verifiable parental consent. The ad networks used the identifiers to target ads to children using HyperBeard's apps. To settle FTC allegations, the company agreed to pay \$150,000 and to delete personal information it illegally collected from children under age 13.
- ▶ [Miniclip, S.A.](#), a Swiss-based company that makes mobile and online digital games, falsely claimed from 2015 through mid-2019 that it was a current member of the Children's Advertising Review Unit's (CARU) COPPA safe harbor program even though CARU terminated Miniclip's membership in 2015. In July 2020, the Commission approved a [settlement](#) to resolve allegations that Miniclip violated Section 5 by misrepresenting its status in a COPPA safe harbor program. As part of the settlement, Miniclip is prohibited from misrepresenting its participation or certification in any privacy or security program sponsored by a government or any self-regulatory organization, including the CARU COPPA safe harbor program. Miniclip is also subject to compliance and recordkeeping requirements.

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 **241 million 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 consumers after they have asked not to be called again, using robocalls to contact consumers to sell goods or services, and calling consumers using spoofed caller ID numbers. Since 2003, the FTC has brought **151 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 510 companies and 404 individuals involved. The 147 cases concluded thus far have resulted in orders totaling more than \$1.8 billion in civil penalties, redress,



or disgorgement, and actual collections exceeding \$290 million. These actions have halted billions of abusive and fraudulent calls that invade consumers' privacy and cause significant economic harm. During the past year, the Commission initiated actions and settled or obtained judgments as described below:

- ▶ Satellite television provider [Dish Network](#) agreed to pay \$210 million to resolve litigation brought by the Department of Justice on behalf of the FTC, as well as the states of California, Illinois, North Carolina, and Ohio, following remand from the Seventh Circuit Court of Appeals on the issue of the civil penalty amount. Dish Network and its dealers violated consumers' privacy by initiating or causing the initiation of tens of millions of calls to phone numbers on the Do Not Call Registry, using pre-recorded messages, and calling consumers who had previously told Dish or its dealers they did not want to receive calls. The civil penalty award included \$126 million penalty for federal violations, which is a record in a DNC case. The remaining penalties were awarded to the states. The settlement came after more than a decade of litigation.
- ▶ In the [Educare](#) action, the FTC and the Ohio Attorney General reached settlements with defendants that ran a fraudulent credit card rate reduction scheme, including four individuals and six corporate entities. One defendant, Globex Telecom, Inc., 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 taken, and first court order obtained, against a VoIP provider. Globex agreed to pay \$1.95 million, which will be used to compensate victims of the scam, and is now required to abide by detailed client screening and monitoring provisions. For example, Globex will not provide VoIP and related services to clients who pay with stored value cards or cryptocurrency, or to clients who do not have a public-facing website or social media presence. In addition, Globex will be required to block any calls made by its clients that appear to come from certain suspicious or spoofed phone numbers, and to terminate their relationship with any telemarketer or other high-risk client that receives three or more USTelcom Traceback Requests (an official industry complaint about unlawful calls) or line carrier complaints in a 60-day period.
- ▶ In [Alcazar Networks](#), the FTC's second case against a VoIP provider, the FTC charged that defendants facilitated tens of millions of illegal telemarketing phone calls, including some calls from overseas, and continued to do so even after learning that customers were using the service to initiate calls to numbers on the FTC's Do Not Call (DNC) Registry and calls displaying spoofed caller ID numbers, including displaying "911." The defendants provided VoIP services to an Indian VoIP provider named E. Sampark, who the Department of Justice later criminally prosecuted for sending tens of millions of scam calls from India-based call centers to victims in the United States. Another Alcazar customer, Derek Bartoli, was previously sued by the FTC for making more than 50 million illegal telemarketing calls using Alcazar's services. The order settling the FTC's complaint against Alcazar and its owner permanently bans the defendants from assisting telemarketers or overseas customers with dialing robocalls or calls to



phone numbers on the DNC Registry—regardless of whether those customers purportedly have permission to do so. In addition, the order requires the defendants to block calls that display the caller ID number as “911,” related emergency numbers, or unassigned or invalid numbers, and to screen current and prospective customers before providing them with VoIP services. The order imposes a \$105,562 monetary judgment against the defendants.

- ▶ As part of Operation Income Illusion, a government crackdown on deceptive income schemes undertaken as scammers worked to leverage pandemic fears, the FTC took action against [Randon Morris](#) and his companies. A federal court granted the FTC’s request for a temporary restraining order against the defendants, who initiated millions of robocalls nationwide to promote sham work-from-home business opportunity programs. The defendants lured consumers into purchasing these programs with false promises that consumers could earn hundreds of dollars a day and claimed an affiliation with Amazon.com where none existed. They also invoked the coronavirus pandemic in robocall messages to prey on consumers who are concerned about working outside of their homes during a national public health crisis. The temporary restraining order stops the defendants’ deceptive sales practices, freezes their assets, and appoints a receiver over the companies.
- ▶ In [Outreach Calling](#), the FTC and the Attorneys General of New York, Virginia, Minnesota, and New Jersey took on a sprawling fundraising operation that allegedly scammed consumers out of millions of dollars. Defendants served as the primary fundraisers for a number of sham charities that were the subject of numerous law enforcement actions. The sham charities claimed to use consumers’ donations to help homeless veterans, retired and disabled law enforcement officers, breast cancer survivors, and others in need. In fact, these organizations spent almost none of the donations on the promised activities. As much as 90 percent of the money raised by the defendants for these sham charities went to the defendants themselves as payment for their fundraising services. What little money the charities did receive was rarely spent on any of their supposedly charitable missions—sometimes less than two percent. The defendants orchestrated the sham charities’ fundraising operations by soliciting donations, writing fundraising materials, and providing other key support to the sham charities. Defendants placed calls misrepresenting how donations would be used, and in many instances, the calls violated consumers’ do-not-call requests. Under their settlements with the FTC and the states, the defendants are permanently prohibited from participating in any charity fundraising, and from deceiving consumers in any other fundraising effort, including for political action committees (PACs). The defendants are required to clearly inform consumers at the time they ask for money that any donations are not charitable and not eligible for tax deductions. In addition, the defendants are subject to significant monetary judgments and are required to surrender assets. The funds being surrendered by the defendants will be paid to the State of New York, which will contribute the funds on behalf of New York, Virginia, and New Jersey to legitimate charities that perform services that mirror those promised by the sham charities.



- ▶ In [Grand Bahama Cruise Line](#), the defendants allegedly made or facilitated millions of illegal calls to consumers nationwide pitching free cruise vacations between Florida and the Bahamas. The defendants' telemarketing operation bought call lists from lead generators that conducted illegal survey robocalls to identify potential customers. In addition to delivering millions of illegal robocalls, the defendants never scrubbed their lists against the agency's Do Not Call Registry and called phone numbers on the Registry. The defendants also illegally called consumers who asked not to be called and used spoofed caller IDs. Settlements with some of the defendants ban them from robocalling, including assisting others in making robocalls. Litigation continues against lead defendant Grand Bahama Cruise Line.
- ▶ The FTC's case against [8 Figure Dream Lifestyle](#), Online Entrepreneur Academy, and their owners shut down a fraudulent money making scheme that used millions of 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. Under the terms of two stipulated final orders, certain defendants are banned from selling money-making methods and others are banned from selling business coaching programs. Nine of the ten defendants are banned from using robocalls for most purposes, including marketing or advertising. In addition, three defendants are prohibited from selling any investment opportunities. The stipulated final orders impose monetary judgments totaling more than \$32 million, which are partially suspended based on the defendants' inability to pay. The defendants have surrendered assets totaling more than \$1.25 million to the Commission.
- ▶ 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 settlement order resolving the FTC's allegations bans the defendants from selling debt relief services and from all telemarketing. It also imposes a judgment of \$13,881,865 against the defendants, which will be partially suspended based on their inability to pay. The amount each defendant pays will be based on the assets they are required to liquidate.
- ▶ In [FTC v. Jasjit Gotra](#), the FTC reached a settlement with lead defendant Jasjit "Jay" Gotra banning him from nearly all outbound telemarketing. Gotra's company, 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. The settlement order also prohibits Gotra from violating the FCRA, and bars him from misrepresenting his affiliation or association with any other business. It imposes a \$9.85 million civil penalty, of which Gotra will pay \$88,000, based on his limited financial resources. In 2019, [Alliance Security](#) itself also agreed to a complete ban on all telemarketing.



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 vendors of personal health records and related entities that aren't covered by HIPAA to notify individuals, the FTC, and, in some cases, the media when there has been a breach of unsecured individually identifiable health information. In May, the Commission issued a [Request for Public Comment](#) as part of the FTC's systematic review of all current Commission regulations and guides. The comment period closed in August, and the FTC is considering next steps.
- ▶ The [Red Flags Rule](#), under the FCRA, 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. The [Card Issuers Rule](#), also under the FCRA, requires that debit or credit card issuers establish and implement reasonable policies and procedures to assess the validity of an address change request if, within a short period of time after receiving the request, the card issuer receives a request for an additional or replacement card for the same account. Together, the Red Flags Rule and the Card Issuers Rule are known as the Identity Theft Rules. In 2018, the FTC announced a regulatory review of the [Identity Theft Rules](#), in which it sought public comment on, among other things, the economic impact and benefits of the Rules and whether and how the Rules might need to be modified. The Commission received comments during the public comment period in 2019, and 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 Commission is reviewing the more than 170,000 submissions received during public comment period.
- ▶ 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. 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. In 2019, the FTC issued a Notice of Proposed Rulemaking and received comments on proposed amendments to both the [GLB Privacy](#) and [Safeguards Rules](#). In July 2020, the Commission held

a [virtual workshop](#) to examine the amendments to the Safeguards Rule, and received public comments. The FTC is evaluating next steps on both Rules.

- ▶ 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 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, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.
- ▶ In 2020, the Commission sought public comment on changes to and effectiveness of [five FCRA Rules](#), and proposed amendments to harmonize the following rules with Dodd-Frank: The [Address Discrepancy Rule](#), which outlines the obligations of users of consumer reports when they receive a notice of address discrepancy from a nationwide consumer reporting agency (CRA); the [Affiliate Marketing Rule](#), which gives consumers the right to restrict a person from using certain information obtained from an affiliate to make solicitations to the consumer; the [Furnisher Rule](#), which requires entities that furnish information to CRAs to establish and implement reasonable written policies and procedures regarding the accuracy and integrity of the information relating to consumers provided to a CRA; the [Pre-screen Opt-Out Notice Rule](#), which 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; and the [Risk-Based Pricing Rule](#), which requires those who use information from a consumer report to offer less favorable terms to consumers to provide them with a notice about the use of such data.

REPORTS AND STUDIES

- ▶ Section 6(b) of the FTC Act authorizes the Commission to conduct wide-ranging studies separate from the agency’s law enforcement authority. Under Section

6(b), the Commission may issue Orders requiring companies to file Special Reports. In December 2020, the Commission issued 6(b) orders to nine [social media and video streaming services](#) requiring them to provide data on how they collect, use, track, estimate, derive, and present personal and demographic information, their advertising and user engagement practices, and how their practices affect children and teens. The orders were sent to Amazon.com, Inc.; ByteDance Ltd., which operates the short video service TikTok; Discord Inc.; Facebook, Inc.; Reddit, Inc.; Snap Inc.; Twitter, Inc.; WhatsApp Inc.; and YouTube LLC. These recipients will be required to file responses to the 6(b) orders. The information that the Commission obtains from these responses will help inform the Commission's mission of protecting consumers and competition in the marketplace.

- ▶ The Commission also filed the following three reports to Congress in 2020:
 - ▶ In its report, [Fair Credit Reporting Act: Efforts to Promote Consumer Report Accuracy and Disputes, Report to Congress](#), the Commission updated lawmakers on the agency's efforts to educate consumers about their rights to dispute and correct errors in their credit reports.
 - ▶ In its report, [Resources Used and Needed for Protecting Consumer Privacy and Security](#), the Commission provided a comprehensive internal assessment measuring the agency's current efforts related to data privacy and security while separately identifying all resource-based needs of the FTC to improve in these areas.
 - ▶ In its report, [FTC's Use of its Authorities to Protect Consumer Privacy and Security](#), the Commission reported 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.

WORKSHOPS

Beginning in 1996, the FTC has hosted 77 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2020, the FTC hosted the following privacy events:

- ▶ [Information Security and Financial Institutions: FTC Workshop to Examine Safeguards Rule](#). In July 2020, the FTC hosted a virtual workshop regarding proposed amendments to the GLB Safeguards Rule, with more than 700 viewers in attendance. Panelists, many of whom are information security professionals at financial institutions covered by the Safeguards Rule, provided empirical data on



the proposed amendments to the GLB Safeguards Rule as part of the federal rulemaking. The archived video and transcripts are available on the [event page](#).

- ▶ [PrivacyCon 2020](#). Also in July 2020, the FTC held the fifth PrivacyCon as a virtual workshop, with almost 2,000 unique viewers in attendance. The sessions focused on research related to health apps, artificial intelligence, Internet of Things devices, the privacy and security of specific technologies such as digital cameras and virtual assistants, international privacy (including the GDPR), and a closing session that touched on miscellaneous privacy and security issues, including usability, security scanner performance, and advertising tracking. The archived video and transcripts are posted on the [event page](#). [PrivacyCon 2021](#) is scheduled for July 27, 2021, and the Commission has issued a [call for research presentations](#).



- ▶ [Data to Go: An FTC Workshop on Data Portability](#). In September 2020, the FTC held a virtual workshop to examine the potential benefits and challenges to consumers and competition raised by data portability, with more than 880 unique viewers in attendance. Data portability refers to the ability of consumers to move data—such as, emails, contacts, calendars, financial information, health information, favorites, friends or content posted on social media—from one service to another or to themselves. Panelists discussed the status of data portability initiatives in the U.S. and across the world, and also provided analysis on what it takes to realize the benefits data portability promises, and how to make it work. The archived video and transcripts are posted on the [event page](#).



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, 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 education and guidance materials developed in 2020 include:

- ▶ **Cybersecurity for Small Business Campaign.** The FTC continues to promote the Cybersecurity for Small Business Campaign at ftc.gov/Cybersecurity and, in Spanish,



at ftc.gov/ciberseguridad. In 2020, the agency collaborated with the Cybersecurity and Infrastructure Security Agency (CISA) in the development of its [Cyber Essentials Toolkit](#). In recognition of Cybersecurity Awareness Month, the FTC presented a webinar about connected devices to the National Cybersecurity Alliance (NCSA) and introduced the revised business guidance [Careful Connections: Keeping the Internet of Things Secure](#). It also joined hosts NCSA and the Identity Theft Resource Center, dozens of local and national government agencies, and cyber education associations in a Twitter chat to raise awareness about cybersecurity. Other outreach about cybersecurity included a virtual presentation at the New England Library Association's conference and a webinar with women small business owners at a tri-state Small Business Administration (SBA) Women's Business Development Center.

- ▶ **Tax Identity Theft Awareness Week.** As part of its 2020 [Tax Identity Theft Awareness Week](#), the FTC hosted outreach events including webinars, telephone town hall meetings, and a Twitter chat to alert consumers, tax professionals, veterans, and small businesses about the ways they can minimize their risk of tax identity theft, and recover if it happens. Working with federal partners throughout the week, including the Department of Veterans Affairs, U.S. Postal Inspection Service, and Internal Revenue Service (IRS), and with organizations like AARP and the Identity Theft Resource Center, the FTC reached more than 13,200 people. These events allowed the FTC and its partners to share information about tax identity theft and imposter scams aimed at getting people's money and their personal information. FTC staff also presented information about tax identity theft to tax professionals and lawyers as part of an IRS working group, and delivered a Tax Security Awareness webinar with the IRS and local Better Business Bureau.
-
- ▶ **Green Lights & Red Flags: FTC Rules of the Road for Business Seminar.** In October 2020, the FTC hosted [Green Lights & Red Flags: FTC Rules of the Road for Business](#), a workshop focused on truth-in-advertising law, data security, social media marketing, and business-to-business fraud. More than 440 business owners and advertising, marketing, and legal professionals registered for the event. Originally planned as a live workshop in Cleveland, the 2020 workshop became the first-ever online session of the popular FTC business seminar series. Co-sponsors included the Ohio Office of the Attorney General, BBB Serving Greater Cleveland, and the Cuyahoga County Department of Consumer Affairs.
-
- ▶ **Identity Theft Program.** When new forms of identity theft and information misuse emerged during the COVID-19 pandemic, the FTC responded with

consumer education and changes to IdentityTheft.gov. For example, in May, the Agency told [people they could get free, weekly credit reports](#) and how to order them. The Agency continues to help consumers handle the financial impact of COVID-19.

The FTC changed the wording on [IdentityTheft.gov](#) to help people report someone's misuse of their information to claim an Economic Impact Payment and [published a blog](#) that explained what to do in case of theft. The FTC later added a button to the [IdentityTheft.gov](#) landing page to make it faster for people to report unemployment benefits identity theft, and [published a blog](#) with advice about what to do if someone got a notice from their state unemployment benefits office or employer about their supposed application for benefits.

Early in 2020, staff distributed identity theft education material through local libraries, and discussed how to respond to the theft during community meetings with a League of Women Voters and congressional staff. Staff shared identity theft information and FTC resources via webinar with professionals who assist identity theft victims, including legal service providers, volunteers for the Senior Medicare Patrol, and staff in a crime victims' resource center. The FTC continued to collaborate with law enforcement agencies by, for example, co-presenting an identity theft training for community non-profits with an attorney general and US Attorney's office, and teaching a state attorney general's office about FTC identity theft resources.

- ▶ **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 2020, the most-read consumer blog posts addressed [how to avoid Social Security Administration imposters](#) and what to do if scammers ask for money or personal information in [exchange for an Economic Impact Payment](#). Other popular posts explained how to [avoid Bitcoin blackmail](#), dodge [text scams posing as package delivery messages](#), and preserve your privacy and data security during the COVID-19 pandemic. Numerous blogs related to COVID-19 explained how to stay safe while [working from home](#) and while [videoconferencing](#); how to [keep children safe during remote learning](#); and what to do if a [thief got unemployment benefits in your name](#).

- ▶ **Business Blog.** The FTC's [Business Blog](#) addresses recent enforcement actions, reports, and guidance. In



2020, there were 55 data security and privacy posts published on the Business Blog. Highlights include two blogs by the Director of the FTC's Bureau of Consumer Protection: one announcing [new and improved data security orders](#), the other [considering the consumer protection implications](#) of artificial intelligence. In 2020, there was also a post analyzing the FTC's [proposed settlement with Zoom](#), which will require the company to honor its security promises and implement a comprehensive program designed to protect

consumers' information. Another post covered a [settlement with a company whose smart locks](#) had security vulnerabilities.

The FTC published several blogs to help businesses protect data and privacy during the pandemic, including [COPPA guidance for edtech companies and schools](#), [videoconferencing tips for business](#), [advice for companies transferring data to the cloud](#), and a review of seven common [scams targeting businesses](#).

- ▶ **Mobile Device Privacy & Security.** In 2020, the FTC published blogs to help consumers protect their personal information while using mobile devices. A February blog warned that people had reported imposters—posing as a bank or friend in need—[using mobile payment apps to steal money](#). The FTC shared a blog post with tips to help parents protect children's privacy when they use apps—this in response to a [settlement with HyperBeard, an app developer that violated the law](#) when it collected personal information from children under age 13.

INTERNATIONAL ENGAGEMENT

Part of the FTC's privacy and data 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. In 2020, Congress renewed the U.S. SAFE WEB Act for another seven years.

A significant part of the FTC's cooperation efforts in 2020 focused on the response to the COVID-19 pandemic. For example, 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 a virtual roundtable on enforcement and the COVID-19 pandemic for enforcement authorities. GPEN includes 69 privacy authorities from 50 countries, with about 400 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, the [FTC played an important role](#) in policy deliberations and projects on privacy and data security internationally, including the global response to the COVID-19 pandemic. For example, the FTC participated in meetings and activities of the Global Privacy Assembly, the APEC Electronic Commerce Steering Group, the Asia-Pacific Privacy Authorities Forum, and the Organisation for Economic Co-operation and Development, providing input on issues ranging from the COVID-19 pandemic to children's privacy and 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, South Korea, Turkey, and members of the European Parliament. Additionally, the FTC conducted technical cooperation exchanges on privacy and cross-border data transfer issues with Bangladesh, Bermuda, India, and Singapore.





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