Privacy & Data Security
Update: 2016

Federal Trade Commission
January 2016 - December 2016

The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the 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. This broad authority allows the Commission 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 Ensure Data Security?

The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule. To date, the Commission has brought hundreds of privacy and data security cases protecting billions of consumers.

The FTC's other 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 work, the FTC's goals have remained constant: to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace.

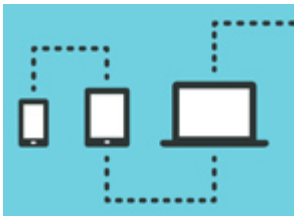
ENFORCEMENT

The FTC has unparalleled experience in consumer privacy enforcement. Its enforcement actions have addressed practices offline, online, and in the mobile environment. It has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies. The FTC's consumer privacy enforcement orders do not just protect American consumers; rather, they protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.

General Privacy

The FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile. These matters include **over 130 spam and spyware cases** and **more than 40 general privacy lawsuits**. In 2016, the FTC announced the following privacy cases:

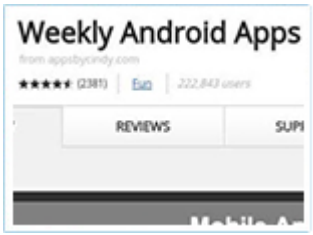
- According to the FTC, until August 2014, operators of the Ashley Madison site lured customers, including 19 million Americans, with fake profiles of women designed to convert them into paid members. The defendants assured users their personal information was private and securely protected but, as described in more detail below, the FTC alleged the security of AshleyMadison.com was lax. According to the complaint, the companies' network experienced a major data breach in July 2015, and in August 2015, the hackers published sensitive profile, account security, and billing information for more than 36 million AshleyMadison.com users. This allegedly included information that the defendants had retained on users who had paid $19 for a "Full Delete" service to purportedly remove their data from the site network. The complaint charged, among other things, that the defendants misrepresented that they had taken reasonable steps to ensure AshleyMadison.com was secure, that they had received a "Trusted Security Award", and that they would delete all of the information of consumers who utilized their Full Delete service. The complaint also charged the defendants with misrepresenting that communications received by members were from actual women when in fact they were from fake engager profiles. The FTC worked with a coalition of 13 states and the District of Columbia to secure a settlement, as well as the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner, who provided assistance to the FTC's investigation and reached their own settlements with the company.
- Mobile ad network Turn Inc. settled FTC charges that it deceived consumers by falsely leading them to believe they could reduce the extent to which the company tracked them online and on their mobile phones. According to the FTC's complaint, Turn told consumers that they could choose not to be tracked by deleting cookies or changing device settings. Despite this, in 2013 Turn joined a Verizon Wireless program in which the carrier added unique identifiers to its users' mobile internet traffic, which allegedly allowed Turn to track millions of Verizon Wireless devices and recreate the cookies on those devices even after an owner deleted them or reset the identifier on their device. In addition, the agency charged that Turn's opt-out mechanism only applied to mobile browsers, and did not block tailored, anonymous ads on mobile applications.



- The FTC brought its first enforcement action against an education lead generator, Gigats.com, settling charges that the company claimed it was "pre-screening" job applicants for hiring employers when it

was actually gathering information for other purposes, including lead generation for post-secondary schools and career training programs. According to the complaint, Gigats.com never sent the information they collected from consumers to employers. Instead, consumers, who had provided Gigats with the kinds of personal information typically requested in a job application, were allegedly directed to call the defendants' "employment specialists," who then steered the consumers toward enrolling in education programs that had paid the defendants for consumer leads.

- Practice Fusion, a cloud-based electronic health record company, agreed to settle charges it misled consumers by soliciting reviews for their doctors, without disclosing adequately that these reviews would be publicly posted on the internet. This resulted in the public disclosure of patients' sensitive personal and medical information, including consumers' full names, medications, health conditions, and treatments received.
- As part of a proposed settlement, Singapore-based mobile advertising company InMobi agreed to pay $950,000 in civil penalties and implement a comprehensive privacy program to settle charges it deceptively tracked the locations of hundreds of millions of consumers – including children – without their knowledge or consent to serve them geo-targeted advertising. The FTC alleged that InMobi mispresented that its advertising software would only track consumers' locations when they opted in and in a manner consistent with their device's privacy settings. According to the complaint, InMobi was actually tracking consumers' locations whether or not the apps using InMobi's software asked for consumers' permission to do so, and even when consumers had denied permission to access their location information.
- Technology company Vulcun settled FTC charges that it unfairly replaced a popular web browser game with a program that installed applications on consumers' mobile devices without their permission. In its complaint, the FTC alleged that Vulcun purchased Running Fred, a Google Chrome browser extension game used by more than 200,000 consumers, and replaced it with Vulcun's own extension, which purported to offer users unbiased recommendations of popular Android applications. What Vulcun's extension actually did, the FTC charged, was to install apps directly on the Android devices of consumers, while bypassing the permissions process in the Android operating system.



- The FTC charged a Florida-based affiliate marketing operation, Tachht, Inc., with bombarding consumers with illegal spam e-mail in an attempt to sell them bogus weight-loss products using false celebrity endorsements. The FTC's complaint alleges that the defendants paid for e-mails to be sent to consumers from hacked email accounts, making it appear to consumers that the messages came from their family members, friends, or other contacts. These email messages lured consumers into clicking on links that led to websites deceptively promoting the defendants' unproven weight-loss products.
- FTC staff issued warning letters to twelve app developers who installed a piece of Silverpush software designed to monitor consumers' television use through the use of "audio beacons" emitted by TVs, which consumers cannot hear but can be detected by the software. The letters warned the app developers that if their statements or user interface state or imply that the apps in question are not collecting and transmitting television viewing data when in fact they do, that the app developers could be in violation of Section 5 of the FTC Act.
- The FTC obtained an order with an individual defendant who operated Sequoia One, a data broker operation that the agency alleged obtained personal information from people who thought they were

applying for payday loans online, and sold it to a scam that tapped consumers' bank accounts and credit cards without their consent. The order prohibits the defendant from selling or disclosing consumers' sensitive personal information, making misrepresentations about any financial or other product or service, and profiting from consumers' personal information and failing to dispose of it properly. It also required the defendant to pay a $45,000 judgment, which represents virtually all his assets.

- The FTC finalized an order against defendant Craig Brittain, the operator of an alleged "revenge porn" website that unfairly and deceptively acquired and posted intimate images of women, then referred them to another website he controlled, where they were told they could have the pictures removed if they paid hundreds of dollars. Under the final order, the defendant is banned from publicly sharing any more nude videos or photographs of people without their affirmative express consent, and must destroy the intimate images and personal contact information he collected while operating the site.
- The First Circuit affirmed the FTC's decision against the operators of Jerk.com, a website that billed itself as "the anti-social network," for deceiving users about the source of content on the website. The Commission found that the operators misled consumers by claiming that content on the website was posted by other users. Instead, most of the content came from Facebook profiles mined by the operators. The Commission also found that the defendants misrepresented the benefits of a paid membership which, for $30, purportedly allowed consumers to update information in their Jerk.com profiles. In fact, consumers who paid for the membership were unable to correct information about them on the site, and did not receive anything of value for their "membership." The First Circuit vacated a requirement that an individual defendant give the FTC updates on his employment status for jobs unrelated to his unlawful activity and remanded to the Commission for further deliberations on this part of the order.

Data Security

Since 2002, the FTC has brought over 60 cases against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk. Significant developments in 2016 included the following:

- In addition to the privacy allegations described above, the operators of the Toronto-based Ashley Madison dating site agreed to settle FTC and state charges that they deceived consumers and failed to protect 36 million users' account and profile information in relation to a massive July 2015 data breach of their network. The site has members from over 46 countries. According to the complaint, the defendants had no written information security policy, no reasonable access controls, inadequate security training of employees, no knowledge of whether third-party service providers were using reasonable security measures, and no measures to monitor the effectiveness of their system security. The settlement requires the defendants to implement a comprehensive data-security program, including third-party assessments. In addition, the operators agreed to pay a total of $1.6 million to settle FTC and state actions.
- The Commission issued a decision and final order concluding that medical testing laboratory LabMD engaged in unreasonable data security practices that resulted in the unauthorized sharing of sensitive medical information. The Commission concluded that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury

and also that the disclosure was likely to cause substantial injury to consumers. The final order requires LabMD to establish a comprehensive information security program subject to assessments and to notify those consumers whose personal information was exposed. LabMD has filed an appeal of the Commission's decision and final order with the Eleventh Circuit Court of Appeals.

- Taiwan-based computer hardware maker ASUS settled Commission charges that critical security flaws in its routers put the home networks of hundreds of thousands of consumers at risk. The FTC's complaint also alleged that the routers' insecure "cloud" services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal information on the internet. Under the final order, ASUS is required to notify consumers about software updates or other steps they can take to protect themselves from security flaws, and establish and maintain a comprehensive security program subject to independent audits for the next 20 years.
- Henry Schein Practice Solutions, the provider of leading office management software for dental practices, agreed to pay $250,000 to settle charges it falsely advertised the level of encryption it provided to protect patient data. The FTC's complaint alleges that Schein marketed its Dentrix G5 software to dental practices around the country with deceptive claims that the software provided industry-standard encryption of sensitive patient information.
- The FTC alleged that Oracle deceived consumers about the security provided by updates to its Java Platform, Standard Edition software (Java SE). According to the complaint, Oracle was aware of significant security issues affecting older versions of Java SE that allowed hackers to craft malware that could give access to consumers' usernames and passwords for financial accounts, and let hackers acquire other sensitive information through phishing attacks. The FTC alleged that Oracle promised consumers that by installing its updates to Java SE both the updates and the consumer's system would be "safe and secure," yet failed to inform consumers that the Java SE update automatically removed only the most recent prior version of the software, and did not remove any other earlier versions. As a result, consumers could still have additional older, insecure versions of the software on their computers that were vulnerable to being hacked. Under the order, Oracle is required to give consumers the ability to easily uninstall insecure, older versions of Java SE.

Credit Reporting & Financial Privacy

The **Fair Credit Reporting Act (FCRA)** sets out rules for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has brought **over 100 FCRA cases** against companies for credit-reporting problems and has collected **over $30 million in civil penalties**. The **Gramm-Leach-Bliley ("GLB") Act** requires financial institutions to send consumers annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties. It also requires financial institutions to implement reasonable security policies and procedures. Since 2005, the FTC has brought **almost 30 cases for violations of the GLB Act**. In 2016, the FTC brought the following case:

- Credit Protection Association, a Texas-based debt collection agency, paid $72,000 in civil penalties and is required to adopt new procedures to settle charges that the company violated the FCRA's Furnisher Rule by not having adequate policies and procedures in place to handle consumer disputes regarding information the company provided to credit reporting agencies. The FTC also alleged that the company

did not have a policy requiring notice to consumers of the outcomes of investigations about disputed information, and that in numerous instances consumers were not informed whether information they disputed had been corrected.

International Enforcement

The FTC enforces key international privacy frameworks, including the EU-U.S. Privacy Shield Framework and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CPBR) System.

The Privacy Shield Framework provides a legal mechanism for companies to transfer personal consumer data from the European Union to the United States. On July 12, 2016, the European Commission issued an "adequacy decision" authorizing data transfers pursuant to the Framework. This enhanced Framework protects consumers' privacy and security through an agreed set of Principles, and gives the FTC a significant role in enforcing these commercial privacy promises. The Framework replaces the U.S.-EU Safe Harbor Program. The FTC brought 39 Safe Harbor cases against companies that violated Section 5 of the FTC Act by making misrepresentations about their participation in that program.

To join the Privacy Shield Framework, a company must self-certify to the Department of Commerce that it complies with the Privacy Shield Principles. A company's failure to comply with the Principles is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts and practices. The FTC has committed to vigorous enforcement of the new Framework, and continues to expect companies to comply with their ongoing obligations with respect to data previously transferred under the Safe Harbor Framework.

The FTC also serves as a privacy enforcement authority in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CPBR) system. The APEC CBPR system is a voluntary, enforceable code of conduct designed to enhance the privacy and security of consumers' personal information transferred amongst the United States and other APEC members. Under the system, participating companies can be certified as compliant with APEC CBPR program requirements that implement the following nine data privacy principles: preventing harm, notice, collection limitation, use, choice, integrity, security safeguards, access and correction, and accountability.

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

- Very Incognito Technologies, a manufacturer of hand-held vaporizers, agreed to settle charges that it deceived consumers about its participation in the APEC Cross-Border Privacy Rules (CBPR) system. The FTC's complaint alleged that the company represented on its website that it was a participant in the APEC CBPR system. Companies that seek to participate in the APEC CBPR system must undergo a review by an APEC-recognized accountability agent, which certifies companies that meet the standards. The company, according to the complaint, was not actually certified.
- The FTC issued warning letters to 28 companies that claim certified participation in the APEC Cross-Border Privacy Rules system on their websites but do not appear to have met the requirements to make that claim. The companies that received the letters must remove the claims regarding APEC CBPR from their websites immediately and inform FTC staff that they have done so, or provide information proving they are actually certified.

Children's Privacy

The **Children's Online Privacy Protection Act of 1998 ("COPPA")** generally requires websites and apps to obtain parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought **over 20 COPPA cases** and collected **millions of dollars in civil penalties**. In 2013, the FTC updated its regulatory rule that implements COPPA to address new developments – such as social networking, smartphone Internet access, and the ability to use geolocation information – that affect children's privacy. (The new rule went into effect July 1, 2013). During the past year, the Commission brought the following case:

- In addition to the privacy allegations described above, the FTC also alleged that mobile advertising company InMobi violated COPPA by collecting this information from apps that were clearly directed at children. The complaint alleged that InMobi's software tracked location in thousands of child-directed apps with hundreds of millions of users without following the steps required by COPPA to get a parent or guardian's consent to collect and use a child's personal information. Under the settlement, InMobi paid a $950,000 civil penalty, was required to delete all information it collected from children, and is prohibited from further violations of COPPA.

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 226 million active registrations. Do Not Call provisions prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry, calling consumers after they have asked not to be called again, and using robocalls to contact consumers to sell goods or services. Since 2003, the FTC has brought 127 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 411 companies and 320 individuals involved. Although a number of cases remain in litigation, the 118 cases that have concluded thus far have resulted in orders totaling more than $147 million in civil penalties and over $1 billion in redress or disgorgement. During the past year, the Commission brought the following cases:

- The FTC, in coordination with the Department of Justice (DOJ), brought a federal court action to stop KFJ Marketing, LLC, a telemarketing operation that allegedly made illegal robocalls promising consumers energy savings, in an effort to generate leads to sell to solar panel installation companies. According to the complaint, the defendants placed more than 1.3 million illegal pre-recorded telemarketing calls to consumers with phone numbers on the national Do Not Call Registry.
- USA Vacation Station settled charges that they made millions of illegal robocalls and calls to numbers on the National Do Not Call Registry to pitch vacation packages. Because the calls were so inexpensive to make, defendants could profitably call more than 100,000 consumers for every vacation package sold. As a result, the defendants bombarded consumers with illegal calls, even after both the Better Business Bureau and the FTC contacted them about their abusive conduct.
- In June, a federal court jury in Utah delivered a verdict in favor of the FTC against Feature Films for Families, Inc., finding that the defendants engaged in deceptive and unlawful telemarketing campaigns

pitching movies, including making more than 117 million illegal calls to consumers, in violation of the FTC's Telemarketing Sales Rule (TSR). The case, which DOJ brought in May 2011 on behalf of the FTC, is the first-ever jury verdict in an action to enforce the TSR and the Commission's Do Not Call Registry rules. The Court has not yet determined the scope of relief.

- The FTC and the Office of the Florida Attorney General charged Life Management Services, Inc. with bombarding consumers with illegal robocalls in an attempt to sell them bogus credit-card interest rate reduction and debt relief services. In all, the complaint alleges the defendants' robocall scheme bilked consumers out of more than $15.6 million since at least January 2013.
- In July, a federal court in Florida granted summary judgment in favor of the FTC against a number of Lanier Law LLC defendants engaged in a mortgage modification scheme. The Court's ruling included a finding that defendants violated the TSR by placing calls to consumers with phone numbers registered on the National Do Not Call Registry and failing to pay the annual fee required to obtain registered phone numbers. Remaining defendants settled with the FTC regarding the same charges.
- The FTC obtained a temporary restraining order and preliminary injunction shutting down Advertising Strategies, LLC, a fraudulent telemarketing scheme that allegedly bilked more than $9 million from thousands of consumers across the nation, many of whom are elderly and live on a fixed income, including military veterans. The defendants are charged with violating the FTC Act and the TSR, including calling numbers on the National Do Not Call Registry.
- A collection of entities known as Consumer Education Group settled charges that they placed more than two million calls, including pre-recorded robocalls, to consumers with phone numbers registered on the National Do Not Call Registry. The defendants created websites that gathered consumer information without obtaining express prior written consent authorizing defendants to call consumers. The FTC, in coordination with DOJ, filed a complaint and settlement imposing injunctive relief and a civil penalty.
- In addition to the cases that the FTC brought directly, in June the Commission led a multinational robocall sweep that took action against operations estimated to be responsible for billions of illegal robocalls and included 39 actions taken by the FTC, the Canadian Radio-television and Telecommunications Commission (CRTC), the United Kingdom's Information Commissioner's Office (ICO), as well as DOJ, the Federal Communications Commission (FCC), the attorneys general offices of Colorado, Florida, Indiana, Kansas, Mississippi, Missouri, North Carolina, Ohio, and Washington State, and the Tennessee Regulatory Authority.

ADVOCACY

When courts, government offices, or other organizations consider cases or policy decisions that affect consumers or competition, the FTC may provide its expertise and advocate for policies that protect consumers and promote competition. In 2016, the FTC filed the following comments related to privacy issues:

- FTC staff filed a comment with the Federal Communications Commission (FCC) on the privacy enforcement implications of the FCC's proposed rulemaking to expand the commercial availability of television set-top boxes for consumers. The comment recommended that if the FCC proceeds with the rulemaking, it should modify the proposed rule to require that third-party set-top box manufacturers also make consumer-facing statements regarding their compliance with certain privacy protections, which could facilitate FTC enforcement pursuant to its authority under the FTC Act.
- The FTC also filed a comment with the FCC regarding the FCC's proposed privacy rulemaking for broadband internet access service providers. The comment offered suggestions regarding the proposed regulatory text based on the FTC's unique experience protecting the privacy and security of consumers' data. The suggested changes addressed a number of issues in the FCC's notice of proposed rulemaking, including how personally identifiable information is defined, the structure of privacy notices, the role of consumer choice in various business practices, and data security and breach notification.
- The FTC filed a comment to the Federal Communications Commission on proposed amendments to the FCC regulations that permit robocalls to collect debt owed to or guaranteed by the federal government without a consumer's prior express consent. The FTC staff comment urged caution with any expansion of permissible robocalling. In the comment, FTC staff outlined the consumer protection concerns raised by these calls and recommended that the FCC create standards for collecting government debt that are consistent with several related laws enforced by the FTC, including the Fair Debt Collection Practices Act (FDCPA) and the Telemarketing Sales Rule. The staff comment proposed that the FCC limit newly-permitted robocalls in four key ways, allowing such calls (1) only to those regarding debts in "default," (2) only to persons who actually owe the debts, (3) only to collect government debt and no other type of debt, and (4) only for collection purposes.
- In response to a request for comment from Department of Commerce's National Telecommunications and Information Administration (NTIA), the FTC filed a comment on the Internet of Things. The comment discussed the benefits and risks of the Internet of Things based on FTC staff's 2015 Internet of Things Report as well as numerous other Commission reports and workshops. In addition, the comment described recommendations for a number of proposed best practices for Internet of Things businesses, including data security. The comment also addressed the role of government in enforcing consumer protections in the Internet of Things, as well as the potential impact on consumers and competition from creating standards that allow various Internet of Things devices to interact and work together.

- FTC staff filed a comment with the National Highway Traffic Safety Administration (NHTSA) regarding its request for comments on proposed industry guidance for highly automated vehicles. The comment commends NHTSA's recommendations designed to ensure that privacy and security issues are considered throughout the vehicle lifecycle, particularly in the design phase.

- The Commission provided testimony to the Senate on the proposed FCC privacy rules for broadband internet access service providers. The testimony highlighted the FTC's extensive history of privacy-related work, and described the FTC's history of partnership with the FCC on various consumer protection issues, including on privacy and data security issues.
- The FTC testified to Congress on its efforts to protect the privacy and security of consumer health information, particularly in areas where health information is being collected, used, and shared outside of doctors' offices or other traditional medical contexts. The testimony provided background on FTC law enforcement efforts, policy work and consumer and business education programs related to health information technology.

RULES

As directed by Congress, the FTC has authority to develop rules that regulate specific areas of consumer privacy and security. Since 2000, the FTC has promulgated rules in a number of these areas:

- The Health Breach Notification Rule requires certain Web-based businesses to notify consumers when the security of their electronic health information is breached.
- The Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.
- The COPPA Rule requires websites and apps to get parental consent before collecting personal information from kids under 13. The Rule was revised in 2013 to strengthen kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13.
- The GLB Privacy Rule sets forth when car dealerships must provide a consumer with a notice explaining the institution's privacy policies and practices and provide a consumer with an opportunity to opt out of disclosures of certain information to nonaffiliated third parties.
- The GLB Safeguards Rule requires financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards. In 2016, the FTC sought public comment on the Rule as part of its systemic review of all current FTC rules and guides.
- The Telemarking 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 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 Do Not Call Registry or who has asked not to receive telemarking calls from a particular company. The Rule also **prohibits robocalls** – prerecorded commercial telemarketing calls to consumers – unless the telemarketer has obtained permission in writing from consumers who want to receive such calls. The Rule was revised in 2016 to prohibit four discrete types of payment methods favored by con artists and scammers.
- 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.
- The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner. In 2016, the FTC sought public comment on the Disposal Rule as part of its systemic review of all current FTC rules and guides. Among other things, the Commission requested comment on whether the definition of "consumer information" should be expanded to include aggregate information or information that can be reasonably linked to an individual.
- The Pre-screen Opt-out Rule under FACTA requires companies that send "prescreened" solicitations of credit or insurance to consumers to provide simple and easy-to-understand notices that explain consumers' right to opt out of receiving future offers.

WORKSHOPS

Beginning in 1996, the FTC has hosted over 35 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2016, the FTC hosted the following privacy events:

- In January, the Commission hosted its first ever PrivacyCon, a conference to examine cutting-edge research and trends in protecting consumer privacy and security. The event brought together leading stakeholders, including whitehat researchers, academics, industry representatives, federal policymakers, and consumer advocates.

- The FTC hosted a three-part Fall Tech Series to examine new and evolving technologies that raise critical consumer protection issues:
  - The first event examined the growing threat of ransomware, discussing how ransomware can infiltrate a system, as well as steps consumers and businesses can take to both prevent infections as well as limit impact. The FTC staff followed up with a blog post providing businesses and consumers with further information on this topic.
  - The second event explored the potential benefits of drones as well as the privacy and security concerns raised by their use, including the practical challenges of providing transparency and choice.
  - The third event focused on how smart TVs may track consumers' viewing habits in new and unexpected ways, as well as best practices for addressing consumer privacy on these systems.
- At the Putting Disclosures to the Test workshop, the FTC convened industry, academics, and policymakers to examine the testing and evaluation of disclosures that companies make to consumers about advertising claims, privacy practices, and other information.

REPORTS AND SURVEYS

The FTC is a leader in developing policy recommendations related to consumer privacy and data security. The FTC has authored **over 50 reports**, based on independent research as well as workshop submissions and discussions, in a number of areas involving privacy and security. In 2015, the FTC released the following:

- Following an earlier FTC workshop, the FTC issued a report entitled Big Data: A Tool for Inclusion or Exclusion? that described some of the laws – including the Fair Credit Reporting Act, the Equal Credit Opportunity Act, and the FTC Act – that address some of the concerns raised by Big Data. The report also outlined a number of questions for businesses to consider to help ensure that their use of big data analytics, while producing many benefits for consumers, avoids outcomes that may be exclusionary or discriminatory.

- In May, the FTC announced that it would study security in the mobile ecosystem. The Commission issued orders to eight mobile device manufacturers requiring them to provide the agency with information about how they issue security updates to address vulnerabilities in smartphones, tablets, and other mobile devices.
- FTC staff issued its "Follow the Lead" Workshop Staff Perspective that discussed the mechanics of lead generation and how it functions in the modern economy. The paper also addressed lead generation's potential benefits as well as the consumer protection issues it raises.
- The FTC announced plans to study data security auditing in the credit card industry. The Commission issued orders to nine companies requiring them to provide the agency with information on how they conduct assessments of companies to measure their compliance with the Payment Card Industry Data Security Standards.
- The Commission released its report on the "sharing" economy in November. Among other things, the report describes potential privacy concerns, and discusses the need for balancing between privacy concerns and the flow of transaction-specific and customer-specific information that is central to the success of the sharing economy.

CONSUMER EDUCATION AND BUSINESS GUIDANCE

Educating businesses and consumers about privacy and data security issues – and how to address related threats – is critical to the FTC's mission. The Commission has distributed **millions of copies of educational materials** for consumers and businesses to address ongoing threats to security and privacy. The FTC has developed extensive materials providing guidance on a range of topics, such as identity theft, Internet safety for children, mobile privacy, credit reporting, behavioral advertising, Do Not Call, and computer security. Examples of such education and guidance materials released in 2016 include:

- The FTC created a web-based tool for developers of health-related mobile apps designed to help the developers understand what federal laws and regulations might apply to their apps. The FTC developed the tool in conjunction with the Department of Health and Human Services' Office of National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR) and the Food and Drug Administration (FDA).
- The FTC launched the enhanced IdentityTheft.gov (robodeidentidad.gov in Spanish), a free, one-stop resource people can use to report and recover from identity theft. Identity theft victims can use the site to create a personal recovery plan, get pre-filled letters and forms to send to credit bureaus and businesses, and create an account to track progress and update their recovery plans. More than 305,000 people have created individual accounts. The FTC's outreach and education during 2016 Tax Identity Theft Awareness Week helped people learn warning signs of tax identity theft, and what to do if they became victims.
- The Commission released new guidance for businesses aimed at giving employment background screening companies information on how to comply with the Fair Credit Reporting Act (FCRA).
- The FTC's Data Breach Response: A Guide for Business, as well as accompanying video and business blog, provide steps that businesses can take and whom to contact in the event of a data breach, as well as a model breach notification letter.

- The FTC's consumer blog alerts consumers to potential privacy and data security harms and offers tips to help them protect their information. In 2016, popular blog posts addressed hacks of wireless routers; faked caller ID; a game that downloaded a security-dodging app; and new data breach video.
- The FTC's Business Blog addresses recent enforcement actions, reports, and guidance. Recent blogs about privacy and data security covered how the National Institute for Standards and Technology (NIST) cybersecurity framework relates to the FTC's long-standing approach to data security; protecting consumer privacy in connected rental cars; additional actions the online advertising industry should be taking to address privacy; the consumer protection implications when a smart product or service, or update and support for it, ends; and advice for ad libraries and for app developers when they consider embedding those libraries into their apps.
- The FTC also hosts a Technology Blog to discuss some of the more technical aspects of the agency's work. For example, last year the FTC posted a blog on technical steps that mobile operating systems have taken to try to address location tracking practices like those alleged in InMobi.

INTERNATIONAL ENGAGEMENT

A key part of the FTC's privacy and security work is engaging with international partners. The agency works closely with foreign privacy authorities, international organizations, and global privacy authority networks to develop robust mutual enforcement cooperation on privacy and data security investigations. The FTC also plays a lead role in advocating for strong, 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. During 2016, the FTC took a major step to enhance privacy enforcement cooperation through its enforcement commitments under the EU-U.S. Privacy Shield Framework, described above. The FTC also entered into the following privacy-related enforcement cooperation arrangements:

- The FTC signed a memorandum of understanding with the Canadian Radio-television and Telecommunications Commission (CRTC) to strengthen cross-border cooperation on Do Not Call and anti-spam enforcement matters. The CRTC enforces the Canadian Anti-Spam Law, which became effective in 2014, while the FTC enforces the FTC Act and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). The MOU recognizes the long-standing partnership between the two agencies, which includes many joint Do Not Call enforcement activities. It facilitates expanded information exchanges and assistance for cross-border Do Not Call and anti-spam enforcement purposes.
- The FTC and 10 international partners signed a memorandum of understanding to facilitate information sharing and enforcement cooperation in the worldwide fight against unsolicited messages and calls. The signing organizations are members of the Unsolicited Communications Enforcement Network (formerly the London Action Plan), a network of public and private-sector entities promoting cooperation to target spam, unsolicited calls, and related problems, such as online fraud and deception, phishing, and dissemination of viruses. The 11 signatories are ACM (the Netherlands), ACMA (Australia), CRTC and OPC (Canada), FTC and FCC (United States), ICO and NTSIT (United Kingdom), KISA (Korea), Department of Internal Affairs (New Zealand), and National Consumer Commission (South Africa).

Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data transferred across national borders. It also works to promote global interoperability among privacy regimes and better accountability from businesses involved in data transfers. During the past year, in addition to participating, alongside the Department of Commerce and other U.S. agencies, in the development of the new EU-U.S. Privacy Shield Framework for transatlantic data transfers, the FTC played a lead role in these international efforts:

- The FTC participated in developing revised guidelines for protecting consumers in e-commerce at the Organization for Economic Co-operation and Development (OECD). The revised guidelines call for businesses to enhance consumer trust in e-commerce by implementing practices relating to the collection and use of consumer data that are transparent and fair, enable consumer participation and choice, and by implementing reasonable security safeguards and digital security risk management measures. The agency also participated, along with other U.S. agencies and stakeholders, in the OECD's Ministerial Meeting on the Digital Economy, addressing emerging privacy issues arising in the Internet of Things and peer platform (sharing economy) marketplaces.
- FTC staff provided technical input and policy advice to agencies on a range of privacy proposals and draft laws, including a staff comment to the Office of the Privacy Commissioner of Canada in its public consultation on the challenges that new technologies and business models pose to consent-based models of privacy protection. The comment recommended that the OPC consider additional enforcement powers that would strongly enhance the OPC's ability to protect and promote privacy in Canada and strengthen the OPC's ability to coordinate with the FTC in cases affecting both Canadian and American consumers.
- Other international engagement included support for the Asia-Pacific Privacy Authorities Forum and Global Privacy Enforcement Network; participation in the International Conference of Data Protection and Privacy Commissioners and the United Nations Committee on Trade and Development's Ad Hoc Expert Meeting on Data Protection and Privacy; and privacy enforcement consultations with authorities from China, Colombia, Ireland, Singapore, the U.K. and others.

Federal Trade Commission
ftc.gov