

ATTACHMENT B

Privacy & Data Security **Update: 2015**

Federal Trade Commission
January 2015 - December 2015



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 notice 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 50 general privacy lawsuits**. In 2015, the FTC announced the following privacy cases:

- ▶ The FTC alleged that defendant [Craig Brittain](#), the operator of an alleged “revenge porn” website, used deception to acquire and post 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 settlement agreement, 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 FTC granted summary judgment 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.”
- ▶ [Nomi Technologies](#), a company whose technology allows retailers to track consumers' movements through their stores, settled charges that it misled consumers with promises that it would provide an in-store mechanism for consumers to opt out of tracking and that consumers would be informed when locations were using Nomi's tracking services. The complaint alleges that these promises were not true because no in-store opt-out mechanism was available, and consumers were not informed when the tracking was taking place.
- ▶ The FTC finalized its order against [TRUSTe, Inc.](#), a provider of privacy certifications for online businesses. The FTC alleged that from 2006 until January 2013, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals in over 1,000 incidences, despite representing on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year.

- ▶ The FTC approved final orders with health billing company [PaymentsMD, LLC](#), and its former CEO, [Michael C. Hughes](#). The FTC charged that they misled thousands of consumers who signed up for an online billing portal by failing to adequately inform them that the company would seek highly detailed medical information from pharmacies, medical labs, and insurance companies.
- ▶ According to the FTC's complaint, data broker [Sequoia One](#) bought payday loan applications of financially strapped consumers, and then sold that information to a scam operation that took millions of dollars from consumers by debiting their bank accounts and charging their credit cards without their consent. As a result, fraudsters obtained the financial account information for more than 500,000 consumers and raided their accounts of at least \$7.1 million.
- ▶ Two data brokers, [Bayview Solutions](#) and [Cornerstone and Company](#), agreed to settle charges that they exposed highly sensitive information – including bank account and credit card numbers, birth dates, contact information, employers' names, and information about debts the consumers allegedly owed – about tens of thousands of consumers while trying to sell portfolios of consumer debt on a public website. The agreements with the FTC require the defendants to abide by strict new requirements to protect consumers' sensitive information.
- ▶ [CWB Services, LLC](#), the operators of a payday lending scheme, are banned from the consumer lending business under settlements with the FTC. The FTC alleged the defendants used personal financial information bought from data brokers to make unauthorized deposits into consumers' bank accounts. After depositing money into consumers' accounts without their permission, the defendants withdrew bi-weekly reoccurring "finance charges" without any of the payments going toward reducing the loan's principal. The defendants then contacted the consumers by phone and email, telling them that they had agreed to, and were obligated to pay for, the "loan" they never requested and misrepresented the true costs of the purported loans.
- ▶ The FTC reached a settlement with [Pairsys, Inc.](#), a company that allegedly tricked seniors and other targeted populations into providing financial information to pay hundreds of dollars for technical support services they did not need, as well as software that was otherwise available for free. Under the terms of the agreement, the defendants are required to turn over multiple real estate properties as well as the contents of numerous bank accounts, and to give up the leases on two luxury cars.
- ▶ The FTC obtained a preliminary injunction against [Click4Support, LLC](#), a tech support scam that allegedly bilked consumers out of more than \$17 million by pretending to represent Microsoft, Apple and other major tech companies. According to the complaint, the defendants used internet advertisements and popups that appeared to be from well-known technology companies to lure consumers into calling them. When consumers called, they were further misled into thinking their computers were riddled with viruses, malware, or security breaches. Consumers were then given a high-pressure sales pitch for unnecessary technical support plans and repair services and defendants obtained their payment information to charge hundreds and sometimes thousands of dollars.
- ▶ Thousands of consumers downloaded the [Prized Mobile app](#), believing they could earn points for playing games or downloading affiliated apps and then spend those points on rewards such as clothes,

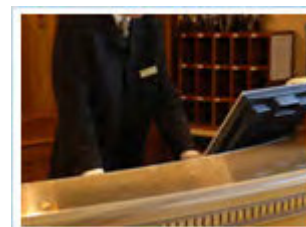


gift cards and other items. The defendant promised consumers that the downloaded app would be free from malware and viruses. However, the FTC alleged that the app's main purpose was actually to load the consumers' mobile phones with malicious software to mine virtual currencies for the defendant. As part of the settlement, the defendant is banned from creating and distributing malicious software, and must destroy all information about consumers collected through the marketing and distribution of the app.

Data Security

Since 2002, the FTC has brought **almost 60 cases** against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk. In 2015, the FTC brought the following cases:

- ▶ [Oracle](#) agreed to settle charges that it 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 allow access to consumers' usernames and passwords for financial accounts, and allow hackers to 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.
- ▶ In [Wyndham Hotels and Resorts](#), the Third Circuit [affirmed](#) the FTC's authority to challenge unfair data security practices using its Section 5 authority. The Third Circuit upheld the District Court's ruling that the FTC could use the prohibition on unfair practices in Section 5 of the FTC Act to challenge the alleged data security lapses outlined in the complaint. The Court also rejected Wyndham's argument that it lacked fair notice that its practices could fall short of that provision.
- ▶ [Wyndham Hotels and Resorts](#) agreed to settle FTC charges that the company's security practices unfairly exposed the payment card information of hundreds of thousands of consumers to hackers in three separate data breaches. Under the terms of the settlement, the company will establish a comprehensive information security program designed to protect cardholder data – including payment card numbers, names and expiration dates. In addition, the company is required to conduct annual information security audits and maintain safeguards in connections between Wyndham's and its franchisees' servers.
- ▶ [LifeLock](#) agreed to pay \$100 million to settle FTC contempt charges that it violated a [2010 settlement with the agency and 35 state attorneys general](#) by continuing to make deceptive claims about its identity theft protection services, and by failing to take steps required to protect its users' data. Specifically, from at least October 2012 through March 2014, LifeLock allegedly violated the 2010 Order by failing to establish and maintain a comprehensive information security program to protect its users' sensitive personal data; falsely advertising that it protected consumers' sensitive data with the same high-level safeguards as financial institutions; and failing to meet the 2010 order's recordkeeping




requirements. The FTC also asserts that from at least January 2012 through December 2014, LifeLock falsely claimed it protected consumers' identity 24/7/365 by providing alerts "as soon as" it received any indication there was a problem.

- ▶ FTC staff sent a [letter to Morgan Stanley](#) closing its investigation into whether the company failed to secure, in a reasonable and appropriate manner, account information related to Morgan Stanley's Wealth Management clients. As discussed in the letter, staff considered several factors in deciding to close the investigation, including the fact that Morgan Stanley had established and implemented comprehensive policies designed to protect against insider theft of personal information.

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 violation of the GLB Act**. In 2015, the FTC brought the following cases:

- ▶ Mobile service provider [Sprint](#) agreed to pay \$2.95 million in civil penalties to settle allegations that the company failed to give proper notice to consumers who were placed in a program for customers with lower credit scores and charged an extra monthly fee. The complaint alleges that Sprint in many cases failed to provide consumers placed in the program with all of the disclosures required by the Risk-Based Pricing Rule, omitting required information that would help consumers understand the information in their credit reports, and that may have alerted them to possible errors that caused them to receive less favorable terms of credit. In addition, the complaint alleges that Sprint often provided these notices to consumers after the window in which they could cancel their service without paying an early termination fee, leaving consumers unable to shop for another carrier that may offer them better terms.
- 
- ▶ The loan-servicing arm of Texas-based auto dealer [Tricolor Auto Acceptance, LLC](#) agreed to pay over \$82,000 in civil penalties as part of a settlement to address charges that it violated the FCRA's Furnisher Rule, which requires companies that report information about consumers to consumer reporting agencies (CRAs) to maintain policies and procedures designed to ensure that the information they report is accurate and to allow consumers to dispute inaccurate information with the company. While the defendant provides information on thousands of consumers to one CRA, the FTC's complaint alleged that the defendant had no written policies or procedures addressing how to ensure the accuracy of that information. The complaint further alleges that when consumers disputed the accuracy of the information provided by the defendant to the CRA, the defendant referred them back to the CRA instead of conducting an investigation as required under the Rule.

U.S.-EU Safe Harbor

The FTC has enforced the U.S.-EU Safe Harbor Framework, which was implemented in 2000 to facilitate the transfer of personal data from Europe to the United States. The FTC brought a number of new cases this year against companies that violated Section 5 of the FTC Act by making misrepresentations about their participation in the program. It also issued final orders against several companies that had previously violated their Safe Harbor promises. In total, the FTC has used Section 5 to bring **39 Safe Harbor cases** since 2009. During the past year, the FTC brought the following cases:

- ▶ The FTC issued final orders against two U.S. businesses, [TES Franchising, LLC](#), and [American International Mailing, Inc.](#), falsely claiming to abide by the Safe Harbor. The FTC's complaints alleged that the companies' websites indicated they were currently certified under the U.S.-EU Safe Harbor Framework and U.S.-Swiss Safe Harbor Framework, when in fact their certifications had lapsed years earlier.
- ▶ Thirteen companies agreed to settle FTC charges that they misled consumers by claiming they were certified members of the U.S.-EU or U.S.-Swiss Safe Harbor Frameworks when their certifications had lapsed or the companies had never applied for membership in the program at all. Seven of the companies allegedly violated the FTC Act by falsely claiming to have a current certification in one or both safe harbor programs when their certifications had actually not been renewed. The companies are:
 - [Golf Connect, LLC](#)
 - [Pinger, Inc.](#)
 - [NAICS Association, LLC](#)
 - [Jubilant Clinsys, Inc.](#)
 - [IOActive, Inc.](#)
 - [Contract Logix, LLC](#)
 - [Forensics Consulting Solutions, LLC](#)

Six of the companies allegedly violated the FTC Act by claiming certification in one or both safe harbor programs when they never actually applied for membership in the programs. The companies are:

- [Dale Jarrett Racing Adventure, Inc.](#)
 - [SteriMed Medical Waste Solutions](#)
 - [Jhayrmaine Daniels \(California Skate Line\)](#)
 - [Just Bagels Manufacturing, Inc.](#)
 - [One Industries Corp.](#)
 - [Inbox Group, LLC](#)
- ▶ The FTC's final order against [TRUSTe, Inc.](#) prohibits the company from making misrepresentations about its certification process or timeline. While the FTC's case, discussed above, did not allege any Safe Harbor violations, the order applies to all of TRUSTe's certification programs, and explicitly includes its U.S.-EU Safe Harbor certification work.

On October 6, 2015, the European Court of Justice issued a judgment declaring as invalid the European Commission's Decision 2000/520/EC of 26 July 2000 on the adequacy of the U.S.-EU Safe Harbor Framework.

U.S. and EU officials are currently discussing the development of an enhanced mechanism that protects privacy and provides an alternative method for transatlantic data transfers.

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 cases:



- ▶ The FTC approved [Riyo Inc.'s](#) proposal for a new COPPA verifiable parental consent method. Riyo uses a two-step process called "face match to verified photo identification" to verify that the person providing consent for a child to use an online service is in fact the child's parent. In the first step, a parent provides an image of their photo identification, such as a passport or driver's license, which is verified for authenticity using various technologies. In a second step, the parent is then prompted to provide a picture of themselves taken with a phone or web camera, which is analyzed to confirm that the photo is of a live person and not a photo of a still photo. The image is then compared to the identification photo using facial recognition technology to confirm whether the person submitting the photo is the one in the identification. The process includes certain privacy safeguards such as requiring encryption and prompt deletion of any personal information that is collected.
- ▶ In its complaint against app developer [LAI Systems](#), the FTC alleged that the company created a number of apps directed to children, and allowed third-party advertisers to collect personal information from children in the form of persistent identifiers. The defendant failed to inform the ad networks that the apps were directed to children and did not provide notice or obtain consent from children's parents for collecting and using the information. The settlement with LAI Systems prohibits the company from further violations of the COPPA Rule, and requires the company to pay a \$60,000 civil penalty.
- ▶ App developer [Retro Dreamer](#) and its principals agreed to pay \$300,000 in civil penalties to settle charges that they violated COPPA. The FTC alleged that the company created a number of apps targeted to children and allowed third-party advertisers to collect children's personal information in the form of persistent identifiers through the apps. One advertising network over the course of 2013 and 2014 specifically warned the defendants about the obligations of the revised COPPA Rule, and also told the defendants that certain of their apps appeared to be targeted to children under the age of 13.

Do Not Call

In 2003, the FTC amended the **Telemarketing Sales Rule** (TSR) to create a national Do Not Call Registry, which now includes more than 222 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 **122 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 384 companies and 306 individuals involved. Although a number of cases remain in litigation, the 114 cases that have concluded thus far have resulted in orders totaling **more than \$144 million in civil penalties and over \$1 billion in redress or disgorgement**. During the past year, the Commission brought the following cases:

- ▶ The FTC filed a complaint against [Lifewatch Inc.](#), claiming that the company used blatantly illegal and deceptive robocalls to trick older consumers throughout the United States and Canada into signing up for medical alert systems with monthly monitoring fees ranging from \$29.95 to \$39.95. Litigation in this matter is ongoing.
- ▶ At the FTC's request, a federal district court temporarily halted the activities of Orlando-based [All Us Marketing LLC \(formerly known as Payless Solutions, LLC\)](#). According to the FTC's complaint, the company has been bombarding consumers since 2011 with massive robocall campaigns designed to trick them into paying up-front for worthless credit card interest rate reduction programs. The court order stops the illegal calls, many of which targeted seniors and claimed to be from "credit card services" and "card member services." The defendants charged consumers up to \$4,999 for their non-existent services.
- ▶ The FTC and 10 state attorneys general sued a Florida cruise company – [Caribbean Cruise Line, Inc.](#) – and its lead generators for illegally sending billions of political survey robocalls to sell cruise vacations. The cruise company and the lead generators have agreed to consent judgments totaling more than \$13 million. Those settlements are awaiting court approval.
- ▶ In [Money Now Funding, LLC](#), the FTC took action against defendants who used illegal telemarketing calls to cheat American and Canadian consumers out of more than \$7 million in a business opportunity scheme. The FTC obtained final judgments that banned the defendants from selling business and work-at-home opportunities and resolved charges that the defendants conned consumers into thinking they could make money by referring merchants in their area to a non-existent money-lending service. Many victims affected by this scam were seniors with limited income and savings.
- ▶ A federal court imposed a \$1.7 million judgment against three defendants who took part in the [Treasure Your Success](#) scheme that used calls to numbers on the Do Not Call Registry and illegal robocalls to pitch bogus credit card interest rate reduction services to consumers struggling with debt.
- ▶ At the FTC's request, a federal court imposed a \$3.4 million judgment against Jason Abraham, a repeat offender, and his company [Instant Response Systems](#), for engaging in a telemarketing scheme that

used deception, threats, and intimidation to induce elderly consumers to pay for medical alert systems they neither ordered nor wanted. The FTC alleged that defendants illegally placed calls to numbers on the Do Not Call Registry to reach elderly consumers – many of whom are in poor health and rely on others for help with managing their finances – and pressure them into buying a medical alert service.

- ▶ As part of its settlement with [Centro Natural Corp.](#), the FTC obtained an order banning the defendants from the debt collection business and telemarketing. According to the FTC’s complaint, the defendants cold-called consumers and threatened them with harsh consequences, such as arrest, legal actions, and immigration status investigations, if they failed to make large payments on bogus debts. The defendants’ telemarketers also pressured and deceived consumers into paying for unwanted products by telling consumers they would “settle” their debt. Centro also regularly cold-called consumers whose phone numbers were on the Do Not Call Registry.
- ▶ In [Sun Bright Ventures LLC](#), the FTC obtained a federal court order that stopped a telemarketing scam that tricked senior citizens into disclosing their bank account numbers by pretending to be Medicare and falsely promising new Medicare cards. The scheme took millions of dollars from victims’ bank accounts without their consent. Under settlements with the FTC, the defendants were banned from selling healthcare-related products and services.
- ▶ In its case against [First Consumers](#), a federal court permanently barred the ringleader of a multi-million dollar fraud that targeted seniors from all telemarketing activities, agreeing with the FTC’s allegations that he violated the FTC Act and the TSR when he illegally withdrew money from U.S. consumers’ accounts and funneled it across the border to Canada. Telemarketers who carried out the fraud allegedly impersonated government and bank officials, and enticed consumers to disclose their confidential bank account information in order to facilitate the fraud. The defendants then used that account information to create checks drawn on the consumers’ bank accounts and deposit them into corporate accounts they established.
- ▶ The FTC announced [the winner of its Robocalls: Humanity Strikes Back contest](#), awarding a \$25,000 cash prize to Robokiller, a mobile app that blocks and forwards robocalls to a crowd-sourced honeypot. This is the fourth contest issued by the agency to challenge technologists to design tools to block robocalls and help investigators track down and stop the people behind them.



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 2015, the FTC filed the following comments related to privacy issues:

- ▶ In a letter to the court-appointed consumer privacy ombudsman for the [RadioShack Bankruptcy proceeding](#), Bureau Director Jessica Rich recommended conditions the court could place on the sale of consumers' personal information to protect their privacy. Specifically, the letter, among other things, recommended that consumers' information not be sold as a standalone asset, but be bundled with other assets. The letter also recommended that consumer information be sold only to another entity that is in substantially the same line of business as RadioShack; that the buyer agree to be bound by the RadioShack privacy policies that were in place when the consumers' data was collected; and that the buyer provide consumers with notice and obtain their affirmative consent before using data in a way that is materially different from the promises RadioShack made.
- ▶ In January 2015, FTC staff submitted [a response to the FCC's request for public comment](#) on whether there are legal or regulatory prohibitions that prevent telephone carriers from offering call-blocking technology. The FTC staff comment outlined the vital need for call-blocking technologies as an integral component to providing subscribers with relief from illegal unwanted calls, and indicated its view that no legal impediments existed to prevent the provision of such services to subscribers.
- ▶ In testimony before Congress, the FTC provided feedback on [proposed data security legislation](#) pending before the Subcommittee on Commerce, Manufacturing and Trade of the House Energy and Commerce Committee. The testimony highlighted the Commission's support for data security legislation overall, and it noted elements of the proposed bill supported by the Commission as well as areas where members of the Commission see room for improvement.
- ▶ The FTC highlighted to Congress its multi-faceted approach to [protecting consumers from unwanted telemarketing calls and illegal robocalls](#) in testimony before the U.S. Senate Special Committee on Aging. The testimony describes how the FTC uses every tool at its disposal to fight illegal robocalls, including aggressive law enforcement, crowdsourcing technical solutions, and robust consumer and business outreach.
- ▶ In its testimony to the Senate Special Committee on Aging, the FTC described its work to [fight tech support scammers](#) who trick people into believing their computer has problems, and then charge them hundreds of dollars for unnecessary, worthless, or even harmful services. The testimony outlined aggressive FTC law enforcement, including work with officials in other countries, and the agency's efforts to educate consumers.
- ▶ The FTC provided feedback on proposed legislation before the Subcommittee on Commerce, Manufacturing and Trade of the House Energy and Commerce Committee to address [privacy and security concerns around the growth of so-called "connected cars."](#) In particular, the testimony stated that the proposed legislation could substantially weaken the security and privacy protections that consumers have today.

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. In 2015, the FTC [proposed an amendment to the GLB Privacy Rule](#) to allow auto dealers that finance car purchases or provide car leases to provide online updates to consumers about their privacy policies as opposed to sending yearly updates by mail.
- ▶ 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 [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 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 telemarketing calls from a particular company. The Rule also **prohibits robocalls** – prerecorded commercial telemarketing calls to consumers – unless the telemarketer has obtained permission in writing from consumers who want to receive such calls. In 2015, following a public comment period, the Commission approved several [amendments to the Telemarketing Sales Rule](#), including a prohibition on four discrete types of payment methods favored by con artists and scammers. The TSR changes stop telemarketers from dipping directly into consumer bank accounts by using certain kinds of checks and “payment orders” that have been “remotely created” by the telemarketer or seller. In addition, the amendments bar telemarketers from receiving payments through traditional “cash-to-cash” money transfers. The TSR changes also prohibit telemarketers from accepting as payment “cash reload” mechanisms.

- ▶ 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.
- ▶ 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 2015, the FTC hosted the following privacy events:

- ▶ The FTC held a workshop entitled [*Follow the Lead*](#) to explore online lead generation in various industries, including lending and education. Consumer “leads” sometimes contain sensitive personal and financial information that may travel through multiple online marketing entities before connecting with the desired businesses. The workshop examined the consumer protection issues raised by the practices of the lead generation industry, and what consumers and businesses should know and do to address them.
- ▶ The FTC hosted a workshop on [cross-device tracking](#) to examine the privacy and security issues around the tracking of consumers’ activities across their different devices for advertising and marketing purposes.



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:


- ▶ FTC staff issued a report on the [Internet of Things](#) that discusses how the principles of security, data minimization, notice, and choice apply in this developing marketplace. The report recommends a series of concrete steps that businesses can take to enhance and protect consumers' privacy and security, as consumers start to reap the benefits from a growing world of Internet-connected devices.



- ▶ The FTC issued a [follow-up study of credit report accuracy](#) that found most consumers who previously reported an unresolved error on one of their three major credit reports believe that at least one piece of disputed information on their report is still inaccurate. The congressionally mandated study is the sixth and final study on national credit report accuracy by the FTC.
- ▶ FTC staff released the results of its [third kids' app survey](#) in a blog. This follow-up survey examined what information kids' app developers are collecting from users, whom they are sharing it with, and what disclosures they are providing to parents about their practices.

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 2015 include:

- ▶ The FTC introduced IdentityTheft.gov (robodeidentidad.gov in Spanish), a new resource to help identity theft victims determine which critical steps to take first. It has detailed advice and helpful resources, including easy-to-print checklists and [sample letters](#). The site also helps users connect to organizations that are critical to recovery: credit bureaus, the Social Security Administration, the IRS and local consumer protection offices.
- 
- ▶ The FTC launched its [Start with Security](#) campaign to provide businesses with more information on data security and help them protect consumers’ information. The initiative includes: [new online and print guidance](#) that draws on lessons learned in more than 50 FTC data security cases; a [series of conferences](#) to provide practical tips and strategies to help startups and developers implement effective data security; a [set of videos](#) that illustrate the lessons of *Start with Security*; and a [website](#) that consolidates the FTC’s data security information for businesses.
 - ▶ The FTC’s [consumer](#) and [OnGuardOnline](#) blogs alert consumers to potential privacy and data security harms, and offer tips to help them protect their information. In 2015, popular blog posts addressed: [data breaches](#) at the Office of Personnel Management; [tech support scams](#); protecting [children’s information](#) after a data breach; coping with a [healthcare records](#) breach; and new FTC videos about responding to [hacked email](#) or an [infected computer](#).
 - ▶ The FTC’s [Business Blog](#) addresses recent enforcement actions, reports, and guidance. Recent blogs about privacy and data security covered: tips for businesses on how the [Fair Credit Reporting Act applies to the hiring process](#); easy-to-implement suggestions for [password security](#); what to expect if a business is the subject of an [FTC data security investigation](#); and considerations for companies using [consumer-generated health data](#).
 - ▶ 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 series on privacy and security in mobile computing, discussing [secure application programming interface \(API\) design](#), [permission-based access controls](#), and [improving permissions systems](#).

INTERNATIONAL ENGAGEMENT

A key part of the FTC's privacy work is engaging with international partners. The agency works closely with foreign privacy authorities, international organizations, and global privacy networks to develop robust mutual enforcement cooperation on privacy and data security investigations and cases. 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 to share information with foreign law enforcement authorities and provide them with investigative assistance by using the agency's statutory powers to obtain evidence in appropriate cases. During 2015, the FTC took several steps to enhance privacy enforcement cooperation:

- ▶ The FTC joined with privacy agencies from seven countries to launch a new information-sharing system – [GPEN Alert](#) – that enables participants to share confidential information about investigations and better coordinate international enforcement efforts. The participants are members of the Global Privacy Enforcement Network (GPEN), an informal network of 59 privacy agencies that promotes cross-border cooperation. In addition to the FTC, the initial participants in the GPEN Alert system are: the Office of the Australian Information Commissioner; Canada's Office of the Privacy Commissioner; Ireland's Office of the Data Protection Commissioner; the Netherlands' Data Protection Authority; New Zealand's Office of the Privacy Commissioner; Norway's Data Protection Authority; and the United Kingdom's Information Commissioner's Office.
- ▶ The FTC also participated in the 2015 [GPEN Sweep, along with 28 other privacy enforcement authorities](#). The sweep centered on the privacy practices of websites and apps popular among kids. The FTC conducted a follow-up survey that examined what information kids' app developers are collecting from users, whom they are sharing it with, and what disclosures they are providing to parents about their practices.
- ▶ In a [Memorandum of Understanding with the Dutch Data Protection Authority](#), the FTC and the Dutch authority agreed voluntarily to engage in mutual assistance and the exchange of information in connection with the enforcement of applicable privacy laws.

Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data that is transferred outside the United States and across other 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 a lead role in these international efforts:

- ▶ The FTC participated in the finalization of the APEC Privacy Recognition for Processors (PRP) program, through which data processors can be recognized as meeting the privacy obligations of data controllers certified under the [Cross-Border Privacy Rules System](#).
- ▶ The [Organization for Economic Co-Operation and Development](#) (OECD) released an update to its 2002 Recommendations on Digital Security. The FTC, together with other U.S. agencies and stakeholders, participated actively in revising the recommendation, which specifically calls for cross-border cooperation on digital security risk management.
- ▶ The FTC participated in transatlantic discussions on improvements to the U.S.-EU Safe Harbor Framework and pursued cases to enforce companies' Safe Harbor commitments. Following an October decision by the European Court of Justice declaring as invalid the European Commission's Decision 2000/520/EC of 26 July 2000 on the adequacy of the U.S.-EU Safe Harbor Framework, the FTC continued to participate in negotiations, together with the Department of Commerce and other U.S. agencies, to develop an enhanced mechanism to protect privacy and provide an alternative method for transatlantic data transfers.
- ▶ Other international engagement included participation at the Asia-Pacific Privacy Authorities Forum; the International Conference of Data Protection and Privacy Commissioners; and the OECD. The FTC also engaged directly with numerous counterparts, including hosting privacy officials from Japan and Korea as part of the State Department's International Visitor Leadership Program, and holding a workshop on privacy enforcement cooperation with consumer authorities in Brazil.



Federal Trade Commission
ftc.gov