Federal Trade Commission
2014 Privacy and Data Security Update[1]

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, including Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and Do Not Call. 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.

1 This document covers the time period from approximately January 2014-December 2014. It will be updated on an annual basis. There is some overlap with previously issued Privacy and Data Security Update, which covered the time period from approximately January 2013-March 2014. See http://www.ftc.gov/reports/privacy-data-security-update-2013.

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

viruses, spyware or other security or performance issues on the consumers' computers. The defendants charged consumers hundreds of dollars to remotely access and "fix" the consumers' computers.

- In Innovative Marketing, Inc., a federal appeals court upheld a district court ruling that imposed a judgment of more than $163 million on an individual defendant for her role in an operation that used computer scareware to trick consumers into thinking their computers were infected with malicious soft-

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.

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 **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 2014, the FTC brought the following cases:

- Baker Tilly Virchow Krause, LLP, an accounting firm;
- BitTorrent, Inc., a provider of peer-to-peer (P2P) file sharing protocol;
- Charles River Laboratories International, Inc., a global developer of early-stage drug discovery processes;
- DataMotion, Inc., a provider of platform for encrypted email and secure file transport;
- DDC Laboratories, Inc., a DNA testing lab and the world's largest paternity testing company;
- Level 3 Communications, LLC, one of the six largest ISPs in the world;
- PDB Sports, Ltd., d/b/a Denver Broncos Football Club, a National Football League team;
- Reynolds Consumer Products Inc., a maker of foil and other consumer products;
- Receivable Management Services Corporation, a global provider of accounts receivable, thn4r97.3101 TmPD

and obtained consumers personal information, including bank account data. Sun Bright then debited consumers' bank accounts without providing a product or service.

- The FTC obtained orders against three deceptive timeshare resale operations, banning them from selling timeshare property resale services. The settlements with Vacation Communications Group, LLC, Resort Property Depot, Inc.; and Resort Solutions Trust, Inc. resolve charges that the companies violated the TSR and lured consumers into paying hefty up-front fees, falsely claiming they had prospective buyers for properties they wanted to sell.
- A federal appellate court upheld a district court ruling that several defendants based in the United States and Canada deceived consumers through a telemarketing scheme designed to sell them phony mortgage assistance and debt relief programs. E.M.A. Nationwide and several other defendants allegedly operated a call center in Montreal that cold-called thousands of U.S. consumers, including those whose an [illegible]MCID

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 2014, the FTC filed the following comments related to privacy issues:

- The FTC filed a comment with the National Highway Traffic Safety Administration (NHTSA) on a proposed initiative that would require all cars to have a vehicle-to-vehicle (V2V) communications system in place by 2019. The FTC's comment noted the significant safety benefits that could result from such systems being implemented and applauded NHTSA's approach to addressing privacy and security risks, such as by designing a V2V system to limit the data collected and stored to only that which serves its intended safety purpose.
- In a comment to the Department of Energy regarding its multistakeholder effort to develop a voluntary code of conduct for smart grid privacy and security, FTC staff commended the group's efforts to develop a code focused on the important principles of transparency, accountability, and consumer choice. Among other things, the staff emphasized the importance of providing privacy disclosures in a clear and conspicuous way, at a just-in-time point, rather than buried in an extensive privacy policy or terms of service.
- FTC staff filed a public comment with the National Telecommunications and Information Administration (NTIA) regarding how developments in "Big Data" affect consumer privacy and the interests reflected in the Administration's Consumer Privacy Bill of Rights. The comment describes FTC staff's support for de-identification, accountability mechanisms, and the "notice and consent" model as vital tools to protect consumer privacy in a Big Data era.

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.
- 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 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 2014, the FTC hosted the following privacy events:

- The FTC held a workshop entitled Big Data: A Tool for Inclusion or Exclusion? to further explore the use of "big data" and its impact on American consumers, including low income and underserved consumers.
- The FTC hosted a three-part Spring Privacy Series to examine the privacy implications of three new areas of technology that have garnered considerable attention for both their potential benefits and the possible privacy concerns they raise for consumers.
    - The first event focused on the privacy and security implications of mobile device tracking, which involves tracking consumers in retail and other businesses using signals from their mobile devices.
    - The second seminar examined alternative scoring products, which are used for a variety of purposes, ranging from identity verification and fraud prevention to marketing and advertising. Because consumers are largely unaware of these scores, and have little to no access to the underlying data that comprises the scores, the event discussed the privacy concerns and questions raised by such predictive scores.
    - The final seminar examined consumers' use of connected health and fitness devices that regularly collect information about them and transmit this information to other entities

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 2014, the FTC released the following:

- The FTC issued Data Brokers: A Call for Transparency and Accountability. The report found that data brokers operate with a fundamental lack of transparency and recommended that Congress consider enacting legislation to make data broker practices more visible to consumers and to give consumers greater control over the their personal information.
- FTC staff issued a report examining mobile shopping apps. The report, What's the Deal? An FTC Study on Mobile Shopping Apps, looked at some of the most popular apps used by consumers to comparison shop, collect and redeem deals and discounts, and pay in-store with their mobile devices. It concluded, among other things, that such apps should more clearly describe how they collect, use, and share consumer data, as well as ensure that their data security promises translate into sound data security practices.

CONSUMER EDUCATION AND BUSINESS GUIDANCE

Educating businesses and consumers about privacy and security issues 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, peer-to-peer file sharing, Do Not Call, and computer security. Examples of such education and guidance materials released in 2014 include:

- The FTC released an updated version of Net Cetera: Chatting with Kids About Being Online, our guide to help parents and other adults talk to kids about being safe, secure, and responsible online. This new version deals with such topics as mobile apps, public Wi-Fi security, text message spam, and offers updated guidance on COPPA.
- For consumers who may have been affected by the recently-announced breaches at major retailers, the FTC posted information online about steps people should take to protect themselves.
- The Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security. This year, people viewed more than 5.4 million pages on OnGuard Online and its Spanish-language counterpart, Alerta en Línea.
- The FTC uses blog posts to alert consumers to potential privacy and data security harms, and offer tips to help them protect their information. The FTC posts to its Consumer Blog as well as to blogs to OnGuard Online and the sites for National Consumer Protection Week and Military Consumer. Some examples include: what people should know about web-cam hackers, including security features to look for in an Internet-protocol camera; how people can protect their sensitive health information; tips on how people can protect themselves if their data is exposed in a data breach; how people can remove malware and secure their computers; privacy threats in photo-sharing apps.
- The FTC also has a Business Center Blog that explains, in plain language, recent enforcement actions, reports, and guidance. Some examples of blogs about privacy and data security include: the announcement of GMR Transcription Services, the FTC's 50th data security settlement; steps that human resources professionals can take to protect sensitive consumer information; and highlights of the latest updates to the FTC's COPPA Rule FAQs.
- The FTC hosted 16 events across the country, along with a series of national webinars and Twitter chats as part of Tax Identity Theft Awareness Week. The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.
- The FTC issued new business guidance about privacy and data security, including updated Frequently Asked Questions for COPPA Rule compliance, as well as guidance for employers conducting background checks.

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 statutory 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 2014, the FTC took several steps to enhance privacy enforcement cooperation:

- In a

manner to "ensure data protection and enable trade through increased transparency, effective enforcement and legal certainty when data is transferred for commercial purposes." The FTC brought several Safe Harbor enforcement actions, described in detail above.