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 wom4(o)-2(1t)-an <1(scn 0.001]9(e)-1(7.8(Inc)8(g)2(e)-0.9(s
a()0( )-3((y-0()p(ug((o)2m.2 Entll4(f)10b0)-1he4dd)10(h3(g)p(ug) <MCTw 0.565 10 BDC /CS0 cs8-(-1(tscn 0.0m [(d)-4307(g-22 T

gift cards and other items.

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.-

W

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, B

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 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

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 consumes,fmimegss(e)6(u)hnies fnem(m)1fcns(fd [t)4(o)r e)-1(a)10()-4(iv)3(rs)2(i)10(tn)-4(k)6(ir

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

INTERNATIONAL ENGAGEMENT

Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data that is transferred outside the U