

THE NATIONAL LAW REVIEW

FTC Releases 2018 Privacy and Data Security Enforcement Update

Friday, March 22, 2019

The Federal Trade Commission, the nation's primary privacy and data security enforcer, recently released its [annual report](#) highlighting its privacy and data security activities for 2018.

The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's primary 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, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and providing robust transparency and choice mechanisms to consumers.

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, the Telemarketing Sales Rule, the Fair Debt Collection Practices Act, and the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. To date, the Commission has brought hundreds of privacy and data security cases.

The report highlights data [privacy enforcement actions](#) in 2018, including shutting down revenge porn website [MyEx.com](#), approving a settlement with peer-to-peer payment service [Venmo](#) over deceptive privacy settings, approving an expanded settlement with [Uber Technologies, Inc.](#) to resolve data security and privacy allegations, and approving a privacy and data security settlement with mobile phone maker [BLU Products, Inc.](#) The FTC also obtained a \$3 million civil penalty against [RealPage, Inc.](#), for violating the Fair Credit Reporting Act by failing to ensure the accuracy of tenant screening information.

The FTC remains committed to protecting children's privacy. The settlements with electronic toy maker [VTech Electronics Limited](#) and online talent site [Explore Talent](#) over allegations that they violated the Children's Online Privacy Protection Act made big news in 2018.

Since 2003, the FTC has brought 140 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 465 companies and 374 individuals involved. The 126 cases that have concluded thus far have resulted in orders totaling over \$1.5 billion in civil penalties, redress, or disgorgement, and actual collections exceeding \$121 million.

During the past year, the FTC initiated actions and settled or obtained judgments that include suing a dietary supplement enterprise which allegedly used illegal robocalls to deceptively market dissolvable oral film strips as effective smoking cessation, weight loss and sexual-performance aids. The FTC alleges that these products did not live up to defendants' claims, and that defendants violated the TSR through their use of harassing robocalls.



Article By [Hinch Newman LLP](#)
[Richard B. Newman](#) FTC Lawyer

[Communications, Media & Internet](#)
[All Federal](#)

The court granted the FTC's motion to temporarily halt the operation's marketing of these products.

Another [action](#) involved the operation of imposter military recruiting websites, such as army.com and navyenlist.com. The agency alleged that defendants violated the Do Not Call provisions of the TSR by placing hundreds of thousands of illegal telemarketing calls to phone numbers on the DNC Registry and by failing to pay required fees. The defendants agreed to settle charges that they targeted people seeking to join the armed forces and tricked them by falsely claiming to be affiliated with the military in order to generate sales leads for post-secondary schools.

The FTC is also committed to enforcing the [EU-U.S. Privacy Shield Framework](#). In 2018, five U.S. companies settled FTC charges that they misled consumers about their participation in the Framework.

In February 2018, FTC staff also released [a report examining security updates](#) issued by mobile phone manufacturers. As part of its public [Hearings on Competition and Consumer Protection in the 21st Century](#) initiative, last year the FTC also hosted hearings on [big data, privacy, and competition](#); competition and consumer protection issues associated with the use of algorithms, artificial intelligence, predictive analytics and data security.

© 2019 Hinch Newman LLP

Source URL: <https://www.natlawreview.com/article/ftc-releases-2018-privacy-and-data-security-enforcement-update>