WHAT WE CAN LEARN FROM THE FTC'S 2017 PRIVACY AND DATA SECURITY UPDATE

The Federal Trade Commission's (FTC's) 2017 Privacy and Data Security Update (the Report) highlights the data privacy and security activities and actions taken by the FTC over the past year—including the numerous enforcement actions taken, workshops conducted, advocacy and policy work developed and guidance released. The enforcement actions discussed in the Report provide valuable insight into the FTC's priorities with respect to privacy and data security in 2018.

PRIVACY & DATA SECURITY

Many of the FTC's actions relating to data privacy focused on informed consent and the adequacy of disclosures. Actions against Lenovo Group Ltd (Lenovo), Uber Technologies Inc. (Uber) and Blue Global, LLC highlight the seriousness of a company's failure to obtain informed consent because of either a failure to disclose data collection and sharing practices or misleading and deceptive disclosures.

In Lenovo, for instance, the FTC and 32 State Attorneys General alleged that Lenovo sold its laptops with preinstalled software that allowed the software developer access to consumers' sensitive personal information transmitted over the Internet. The FTC alleged, among other things, that Lenovo's failure to disclose and obtain consent in connection with the software developer's access, collection and transmission of consumer information was an unfair and deceptive practice that violated Section 5 of the FTC Act.

THE BOTTOM LINE

The FTC exercises broad reach over privacy and data security issues across numerous industries. The Report shows a continuing trend towards more enforcement actions and increased penalties. All companies should review their privacy and data practices to confirm that they are in compliance with applicable law, including with respect to consumer-facing disclosures and internal data security practices.

The FTC has also been cracking down on phantom debt collection schemes, which it views to be growing and pernicious problem. The FTC recently brought actions against six companies and three individuals who used a variety of business names such as Stark Law, Stark Recovery and Capital Harris Miller & Associates that pressured consumers nationwide for money that they did not owe. The operations sold fake "debt portfolios" that included personal and other sensitive information to other collection companies, who would then contact innocent consumers. Victims had entered personal information into fake loan websites operated by these companies and did not know that their information was being sold.

Significant enforcement actions in the area of data security focused on inadequate security practices. For example, in the action against Uber, the FTC's complaint alleged that Uber failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases Uber stored with a third-party cloud provider. Uber did not require its engineers and programmers to use distinct access keys to access personal information stored in the cloud, or require multi-factor authentication to be used, and full administrative access was provided

>> continues on next page

to all engineers and programmers. Sensitive information was also stored in plain readable text in database backups. As a result of this lax security, an intruder was able to access over 100,000 names, driver's license numbers and other information stored by Uber. In a similar action against D-Link Corporation (D-Link), a computer networking equipment manufacturer, the FTC alleged that D-Link failed to take steps to address well-known and easily preventable security flaws, leaving its products vulnerable to attack.

CREDIT REPORTING AND FINANCIAL PRIVACY

Over the years, the FTC has collected over $30 million in civil penalties from companies for violating the Fair Credit Reporting Act and has brought numerous cases against financial institutions under the Gramm-Leach Bliley Act (GLBA). The Report highlights the FTC's continued enforcement efforts in the financial and credit reporting industries in 2017. In particular, the FTC brought an action against TaxSlayer LLC (TaxSlayer) for violating the Safeguards Rule of the GLBA by failing to develop a comprehensive security program and implement safeguards to protect customer information. Because TaxSlayer did not have adequate risk-based authentication measures that would have reduced hacking, and did not require customers to choose strong passwords, malicious hackers gained access to nearly 9,000 TaxSlayer accounts and filed fraudulent returns to obtain tax refunds. The FTC also alleged that TaxSlayer failed to deliver clear and conspicuous initial privacy notices in a way that ensured customers received the notice, as required by the Privacy Rule and Regulation P of the GLBA.

CHILDREN'S PRIVACY

The FTC has brought over 20 cases and collected millions in civil penalties for violations of the Children's Online Privacy Protection Act of 1998 (COPPA) since 2000. In a new policy enforcement statement released by the FTC in 2017, the FTC provided additional guidance on how COPPA applies to the collection of audio voice recordings.

COPPA requires websites and online services directed to children to obtain verifiable parental consent before collecting audio recordings of a child's voice, a practice that raised questions about the applicability of this requirement to the collection of a child's voice for the sole purpose of instructing a command or request on Internet-connected devices. The FTC agreed that it would not take action against an operator for failing to obtain verifiable parental consent if a child's voice is collected solely as a replacement of written words, such as to perform a search or to fulfill a verbal instruction or request, so long as it is only held for a brief time.

In 2017, the FTC also approved proposed modifications by TrustArc (formerly TRUSTe) to its safe harbor program under COPPA, including the addition of a new requirement that participants conduct an annual internal assessment of third-parties' collection of personal information from children on their websites or online services.

DO NOT CALL

Since the creation of a national Do Not Call Registry in 2003, there have been over 130 cases brought to enforce the Do Not Call provisions against telemarketers, and over $1.5 billion in civil penalties, redress or disgorgement have resulted from the concluded cases. In 2017, the FTC continued its siege on violators. For instance, as a result of litigation brought by the U.S. Department of Justice on behalf of the FTC and four states, the federal court ordered penalties totaling $280 million and strong injunctive relief against Dish Network for violations of FTC's Telemarketing Sales Rule, including Do Not Call and abandoned call violations, the Telephone Consumer Protection Act and state laws. Similarly, the FTC and ten state partners obtained a final order against Caribbean Cruise Line for its illegal robocall and telemarketing

>> continues on next page

practices. The FTC also obtained settlement orders with individual leaders of several telemarketing operations that blasted illegal robocalls to consumers and called numbers listed on the Do Not Call Registry.

INTERNATIONAL ENFORCEMENT

In addition to policing privacy and security practices domestically, the FTC is also tasked to enforcing several key international privacy frameworks. Last year, the FTC brought its first three enforcement actions under the EU-U.S. Privacy Shield and participated in the first Annual Review of the Privacy Shield's framework. The FTC also carried out four enforcement actions under the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System.

FOR MORE INFORMATION

Gary A. Kibel
Partner
Digital Media, Technology & Privacy
212.468.4918
gkibel@dglaw.com

Allison Fitzpatrick
Partner
Advertising, Marketing & Promotions
212.468.4866
afitzpatrick@dglaw.com

Justin H. Lee
Associate
Digital Media, Technology & Privacy
212.468.4894
jlee@dglaw.com

Vivian Wang
Associate
Digital Media, Technology & Privacy
212.468.4927
vwang@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com