THE PRIVACY ADVISOR

What FTC Enforcement Actions Teach Us About the Makings of Reasonable Privacy and Data Security Practices

A Follow-Up Study

By Müge Fazlioglu, CIPP/E, CIPP/US

11 June 2018

In this report, we update our September 2014 study, "What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices," originally written by IAPP Westin Fellow Patricia Bailin, CIPP/US, CIPM, CIPT, now head of privacy at Datavant. The initial study analyzed organizational failures on issues of privacy, security, software/product review, service providers, risk assessments, unauthorized access/disclosure, and employee training. Moreover, the study described the specific obligations mandated in each settlement, such as performing risk assessments, obtaining explicit consent from users, imposing access limitations, building encryption protocols into security policies, and performing reviews and testing of software security and products.

The initial study covered FTC complaints filed between 2002 and August 2014 (the most recent case it examined involved GMR Transcription Services, Inc., a settlement released August 14, 2014). The present study encompasses all subsequent complaints, that is, those published between August 15, 2014, and May 15, 2018. By searching the IAPP's FTC Casebook, we identified 50 relevant cases. Only complaints against and settlements with incorporated and limited liability companies were included in the analysis (i.e., cases with an individual person named as the defendant were not considered).

The original study advanced those seven non-mutually exclusive categories to suggest "possible guidelines for complying with FTC privacy and data security standards based on what the FTC

has determined inadequate." This study builds upon these categories and provides additional insights into the FTC's standards by examining complaints and settlements involving companies that collected consumers' personal or sensitive information without providing notice and/or obtaining consent, disclosed consumers' personal or sensitive information, failed to protect against unauthorized access to data, misled consumers about privacy and/or data security, made false claims about participating in international privacy agreements, or engaged in other deceptive practices involving privacy. The following sections review the relevant complaints and settlement orders while explaining the steps companies can take to comply with the FTC's privacy and data protection standards as inferred from these cases.

Collecting consumers' personal and/or sensitive information without notice and consent

The largest number of FTC complaints in this area from 2014 to 2018 were directed at companies that failed to adequately notify consumers what information they were collecting about them and/or to obtain consent from them prior to collection. Notice and choice constitute the foundational twin pillars of privacy protection in the U.S. Despite the challenges they present, these concepts remain central to contemporary privacy law. Companies that fail to accurately notify customers about the information they collect about them or to obtain their consent prior to collection risk running afoul of the FTC's jurisdiction against "unfair or deceptive acts or practices."

In two of the three FTC settlement orders that required a company to implement a comprehensive privacy program, the violator had allegedly tracked consumer activities without notifying them or obtaining their consent to do so. In its complaint against VIZIO, the FTC contended that the company had "comprehensively collect[ed] the sensitive television viewing activity of consumers … [and] provided this viewing data to third parties … through a medium that consumers would not expect to be used for tracking, without consumers' consent." Similarly, the FTC's complaint against InMobi Pte alleged that the Singaporean company, a subsidiary of the Indian-headquartered InMobi, had tracked consumer locations for use in geo-targeted advertising, absent both notice and consent. Regardless of consumers' device settings, InMobi allegedly tracked their location through the iOS location application programming interface (known as an "API") and from the WiFi networks to which a consumer's device was connected, but misrepresented these facts to its consumers as well as its business partners. Moreover, while thousands of applications that used InMobi's software had indicated to the company that their products and services were targeted at children, InMobi allegedly failed to notify the children's parents or receive their consent in violation of the Children's Online Privacy Protection Rule.

Several more complaints involved unlawful collection of information without adequate notice and consent. For example, a medical payment services company, PaymentsMD, was the subject of an FTC complaint alleging that it failed to disclose to consumers that it was seeking and collecting their sensitive health information from pharmacies, health plans, and laboratories, about things such as what medication(s) they were on, their laboratory test results, and medical procedures performed on them. App-maker Vulcun settled with the FTC over a complaint that it installed an app on users' android mobile devices "without adequately disclosing to users that

the software would be installed." Vulcun had acquired a popular browser-based game, replaced it with their own program, and installed additional apps on users' mobile devices.

The inferred FTC's standards around collecting consumers' information:
The cases outlined above offer several guidelines for companies seeking to comply with the FTC's standards for privacy and data protection as articulated therein. Based on the complaints against VIZIO and InMobi, a company should:

- "[A]dequately disclose" features of its products that comprehensively collect and share consumers' data and obtain consumers' prior consent for such collection.

In PaymentsMD, consumers were asked to check a box to consent to the statement that, "health records related to your treatment … may be used or disclosed …" The FTC found this consent form inadequate due to the way it was presented to consumers. A company should ensure that in designing a website to obtain consent it:

- Does not make it "hard to read the authorizations in their entirety," and does not make it "easy to skip over them by clicking a single check box" preceding all authorizations.

A company engaged in the collection of health or other sensitive information from third parties should:

- "[C]learly and prominently" disclose to consumers its practices involving the "collection, use, storage, disclosure or sharing" of information, and obtain consumers' "affirmative express consent" prior to gathering sensitive information from a third party.

In other words, companies seeking to obtain consumers' sensitive information should clearly present in the consent agreement that consumers are giving the company permission to do so.

Although it had a screening mechanism to prohibit users under age 13 from registering on its website, the FTC found that Yelp "failed to implement a functional age-screen mechanism in the new in-app registration feature" and accepted registrations from users who input dates of birth that indicated they were under the age of 13. Central to the FTC's complaint against Yelp was the finding that it failed to test the age-restriction aspect of its iOS and Android apps.

Thus, it is vital that a company seeking to comply with COPPA:

- Does not merely implement privacy controls, but test the implemented controls to confirm that they function as intended.

FTC standards regarding the collection of information from children can also be inferred from several cases the agency brought against companies for violating the COPPA Rule, including TinyCo, VTech, LAI Systems, Retro Dreamer, and Prime Sites/Explore Talent. Given these types of complaints, companies' privacy policies for online services that collect information from children should give "clear, understandable, and complete notice of their information practices." Companies should also provide notice to and obtain consent from parents prior to

"collecting, using, and/or disclosing personal information from children." Moreover, a company seeking to collect information from children should:

- Make "reasonable efforts, taking into account available technology," that parents receive direct notice of the information about children it is collecting, using, or disclosing.
- Post a "prominent and clearly labeled link" to its information practices regarding children on the homepage of its website and at each place where personal information from children is collected.
- Obtain "verifiable parental consent" before collecting, using, or disclosing any child's personal information.
- Follow "reasonable procedures" so that the confidentiality, security, and integrity of personal information is protected.

Lastly, the FTC's decision and order for Vulcun implies that prior to offering or making a "material change" to an existing product or service, a company must:

- "[C]learly and conspicuously" disclose the types of information its products or services would access and how that information would be used as well as "[t]he nature of any material change" to its products or services.
- Display a built-in notice or approval request for the installation of products or services.
- Obtain a consumer's "express affirmative consent" prior to installing or making any material changes to a product or service.

Disclosing consumers' personal and/or sensitive information

In addition to the unlawful collection of personal information, the FTC also has taken several actions against companies that unlawfully disclosed consumers' personal information. Debt brokers Cornerstone and Company and Bayview Solutions were both charged by the FTC with "unfair public disclosure of consumers' sensitive personal and financial information" in violation of Section 5 of the FTC Act. The FTC alleged that the companies posted debt portfolios for sale on their websites in the form of "unencrypted, unprotected Excel spreadsheets" that contained information on tens of thousands of individuals, including their amounts of debt, first and last names, dates of birth, addresses, telephone numbers, bank account numbers, and driver's license numbers.

In a similar complaint involving the unlawful public exposure of sensitive information, the FTC charged Wyndham Worldwide Corporation with "engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."

Practice Fusion also reached a settlement with the FTC over charges that it misled consumers about their personal information being posted on a public website. A cloud-based electronic health record service, Practice Fusion allowed patients to download and transfer health information and send and receive messages from their providers. To generate reviews, Practice Fusion solicited information from patients following a visit with their provider through an online survey, which included a text box where patients could write up to 255 characters.

Although the form included a pre-checked box that said, "Keep this review anonymous," the FTC explained in its complaint that checking this box "did not anonymize anything a consumer wrote in the free text box, including a consumer's identifying information." These reviews often contained sensitive information, such as medical conditions, treatments, and prescriptions, combined with personally identifying information, such as full names and telephone numbers. Moreover, the FTC found that the website did not contain "any historical or contextual reference to alert them to the fact that their feedback would be publicly posted rather than provided to their physician."

The inferred FTC's standards around disclosing consumers' sensitive or personal information:

In the complaints against Cornerstone and Company and Bayview Solutions, the FTC stated affirmatively what these companies should have done "at virtually no cost" to avoid public disclosure of consumers' sensitive personal information. The agency suggested the defendants should have acted by redacting, encrypting, and password-protecting the Excel spreadsheet, or "offering to make the information available through other secure means."

In the settlement orders, both companies were required to implement information security programs, which involved identifying the "material internal and external risks to the security, confidentiality, and integrity" of personal information. Furthermore, the FTC required the companies to conduct risk assessments to consider risks in at least the following areas:

- Employee training and management.
- Information systems, including network and software design, information processing, storage, transmission, and disposal.
- Prevention, detection, and response to attacks, intrusions, or other system failures.

In addition, the information security programs were required to include "the design and implementation of reasonable safeguards to control the risks identified through risk assessment," and to evaluate and adjust the programs in line with the results of these required testing and monitoring obligations.

In its settlement order, Wyndham was also required to implement a comprehensive information security program, similar to the programs required of Cornerstone and Company and Bayview Solutions. Furthermore, based on the details provided in the FTC's complaint against Wyndham, companies should:

- Use "readily available security measures," such as firewalls, to limit access between management systems, the corporate network, and the internet.
- Ensure that software is appropriately configured (e.g., do not allow storage of sensitive data in clear readable text).
- Implement "adequate" information security policies and procedures prior to connecting any local computer networks to the company network.
- Remedy any known security vulnerabilities on servers connected to the company network (e.g., by not allowing insecure servers to connect to the network or using "outdated operating systems" incapable of receiving security updates or patches).

- Prohibit the use of well-known default user IDs and passwords on servers connected to the company network and employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess.
- Monitor and manage computers connected to the company network.
- Employ "reasonable" measures to detect and prevent unauthorized access to the company network and conduct security investigations.
- Follow appropriate incident response procedures, such as monitoring the company network for malware.
- Adequately restrict third-party vendor access to the company network and management systems (e.g., by restricting connections to specified IP addresses or granting temporary, limited access on an as-needed basis).

Finally, given the FTC's complaint against and settlement with Practice Fusion, companies should be sure to "clearly and conspicuously disclose to the consumer, separate and apart from 'privacy policy,' 'terms of use' page, or similar document," when individually identifiable or health information given by an individual is being made publicly available and obtain that person's affirmative express consent before doing so.

Failing to protect against unauthorized access to data

A group of FTC complaints from 2014 through 2018 involved deceptive or unfair data security practices. Among other things, the FTC ordered companies that were found to have inadequate protections against unauthorized access to data to implement comprehensive privacy or data security programs, including risk assessments. This line of cases includes ASUSTeK Computer, Life Inc. (owner of the AshleyMadison.com website), TaxSlayer, Uber Technologies, Lenovo, and LabMD.

The case of Life Inc. ("Ruby Corp.," owner of the AshleyMadison.com website), which settled in December 2016, involved a data breach in 2015 that exposed the profile information of 36 million of the site's users. The FTC's complaint stated that, despite claims that the website was "100% secure," "risk free," and "completely anonymous," the company "engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to personal information on their network." The complaint concluded that, "[i]n truth and in fact … [Ruby] did not take reasonable steps to ensure that AshleyMadison.com was secure."

As a financial institution that processes customer information, TaxSlayer was already subject to the Safeguards Rule, which requires such companies "to develop a written information security plan that describes their program to protect customer information." Its lack thereof, as well as its failure to conduct a risk assessment or implement information safeguards, contributed to its vulnerability to a list validation attack, in which remote hackers gained access to 8,882 TaxSlayer accounts and used that information to engage in tax identity theft.

The FTC's complaint against TaxSlayer documented its failure to comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act. In the final decision and order, TaxSlayer was restrained and enjoined from violating any provision of the Privacy Rule or the Safeguards Rule and required to implement a data security program.

Uber Technologies, Inc. was also the subject of an FTC complaint for failing to monitor access, failing to provide reasonable security, and making deceptive privacy and data security claims. Uber initially agreed to settle with the FTC in August 2017, and agreed to an expanded settlement in April 2018. The decision and order for Uber required it to implement a "comprehensive privacy program" to address risks and safeguard personal information.

Lenovo settled with the FTC over a complaint that it had compromised the security of consumers' laptops by pre-installing advertising software on its hardware. Lenovo was ordered to give customers a "reasonable and effective means ... to opt out, disable or remove all of the ... software's operations," and mandated to implement a "comprehensive software security program" to address risks and protect information.

The FTC's complaint against ASUSTeK Computer Inc. involved the company's alleged failure to secure the software used in its routers. In the most recent case analyzed in this study, the FTC filed a complaint against cell phone company BLU Products for causing software to be installed on consumers' devices that transmitted personal information about them — including the full contents of their text messages, cell tower location data in real-time, contact lists, and a list of applications installed and used on their device — to a third-party without consumers' knowledge or consent. As in the previously discussed cases, ASUSTeK and BLU were required to implement comprehensive data security programs.

Two companies charged with data security failures stand out for not having reached a final settlement with the FTC. A judge initially dismissed the FTC's complaint against LabMD, a clinical testing laboratory, which allegedly failed to provide reasonable and appropriate safeguards against unauthorized access to consumers' personal information. The judge wrote that, at best, the complaint proved the "possibility," not the "probability or likelihood" of harm. In July 2016, the FTC overturned the judge's ruling. On appeal, the 11th Circuit found the FTC's order to lack "specificity" and thus to be "unenforceable," arguing it would have put the district court "in the position of managing LabMD's business in accordance with the Commission's wishes."

In January 2017, the FTC filed a complaint against D-Link Corporation for its failure to take adequate security measures that left its wireless routers and Internet cameras vulnerable to hackers. D-Link, however, filed a motion to dismiss. Several parts of the complaint, on appeal, were dismissed because the FTC could only demonstrate "the mere possibility of injury at best." While the judge gave the FTC the option to file an amended complaint, and the the case is ongoing in California.

The inferred FTC's standards around failures to protect against unauthorized access to data:

In this line of cases, the FTC has mandated that companies implement a "comprehensive security program that is reasonably designed to address security risks" and "protect the privacy, security, confidentiality, and integrity" of consumers' information. These programs have all included conducting a risk assessment of "material internal and external risks" to the security of devices and to personal information "that could result in the unintentional exposure of such information by consumers or the unauthorized disclosure, misuse, loss,

alteration, destruction, or other compromise of such information." These risk assessments have been required to consider risks in various areas, including:

- Employee training and management, including in secure engineering and defensive programming.
- Product design, development and research.
- Secure software design, development and testing, including for default settings, access key, and secret key management and secure cloud storage.
- Application software design.
- Information systems, such as network and software design, information processing, storage, transmission, and disposal.
- Review, assessment, and response to third-party security vulnerability reports, including a "bug bounty" or similar program.
- Prevention, detection, and response to attacks, intrusions, or other system failures or vulnerabilities.

Following the identification of risks, companies must also:

- Design and implement "reasonable safeguards" to control the identified risks.
- Conduct regular testing of the effectiveness of key controls, systems, and procedures.
- Evaluate and adjust their information security program based on the results of the testing or based on "any other circumstance" the company "knows or has reason to know may have a material impact on [its] effectiveness."
- Take "reasonable steps" to work with service providers capable of protecting personal information and require them by contract to implement appropriate safeguards.

Furthermore, based on the FTC's decision in the AshleyMadison.com case, companies should also take the following steps:

- Have a written organizational information security policy.
- Train personnel to adequately perform data security-related tasks and responsibilities.
- Ensure that third-party service providers implement reasonable security measures to protect personal information, such as through the use of contractual obligations.
- Use readily available security measures to regularly monitor systems and assets to identify data security events and verify the effectiveness of protective measures.
- Keep track of unsuccessful login attempts.
- Secure remote access.
- Revoke the passwords of former employees of their service providers.
- Restrict access to data systems based on an employee's job functions.
- Not allow employees to reuse passwords to access different servers and services.
- Deploy reasonable controls to prevent the retention of passwords and encryption keys in clear text files on the company's network.

Lastly, as mandated in ASUSTeK, companies seeking to design and implement "reasonable and appropriate software security testing techniques" should consider:

- Vulnerability and penetration testing.
- Security architecture reviews.
- Code reviews.
- Other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to devices and information is restricted consistent with a user's security settings.

Misleading consumers about privacy and data security

A large number of enforcement actions have been brought by the FTC against companies that made misleading statements about their privacy practices. For example, TRUSTe was the subject of an FTC complaint after it allegedly represented that it annually recertified companies that displayed its Privacy Seal, despite having failed to do so in more than 1,000 instances. TRUSTe agreed to a settlement whereby it would refrain from misrepresenting "[t]he steps it takes to evaluate, certify, review, or recertify a company's privacy practices," and also agreed to pay a fine of $200,000. Similarly, retail tracking firm Nomi Technologies was charged by the FTC with falsely claiming that consumers could opt-out of its tracking activities and that consumers were provided notice of such tracking. It was subsequently ordered not to make such misrepresentations.

Making misleading claims about data security also made companies the target of FTC enforcement actions. Henry Schein Practice Solutions, a dental practice software company, agreed to settle a complaint with the FTC over allegations that it mislead customers about the encryption of data. In another case, Oracle was the subject of an FTC complaint over its claims about updates to its Java Platform, Standard Edition. When consumers downloaded updated versions of Java SE, only the most recent prior iteration of the software was removed, potentially leaving older, less secure versions on consumer's devices. Despite allegedly being aware of these vulnerabilities, Oracle failed to disclose this information to consumers during the update process.

The inferred FTC's standards around misleading consumers about privacy and data protection:

Based on an analysis of the above cases, companies must be careful to not misrepresent the privacy or security of their software, such as "whether or to what extent" its product "offers industry-standard encryption." Companies should also notify customers if they use "a less complex encryption algorithm to protect patient data than Advanced Encryption Standard ('AES'), which is recommended as an industry standard by the National Institute of Standards and Technology ('NIST')." Moreover, based on the settlement order Oracle agreed to, companies should provide "[c]lear and [c]onspicuous" notifications to consumers that may have older, insecure iterations of software on their devices, along with instructions on how to remove them.

Making false claims about participating in international privacy agreements

The FTC pursued several companies for allegedly making false claims regarding their participation in international privacy agreements, including the U.S.-EU Safe Harbor

Framework, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system, and the EU-U.S. Privacy Shield.

TES Franchising, American International Mailing, Golf Connect, Pinger, NAICS Association, Jubilant Clinsys, IOActive, Contract Logix, Forensics Consulting Solutions, Dale Jarrett Racing Adventure, SteriMed Medical Waste Solutions, California Skate-Line, Just Bagels Mfg., One Industries Corp., and Inbox Group were all charged with making false claims about their participation in the U.S.-EU Safe Harbor Framework, and were prohibited from further misrepresenting their participation in any government-sponsored or self-regulatory privacy or data security program. Three other companies, DecuSoft, Tru Communication, and Md7, settled with the FTC over charges that they allegedly misled consumers regarding their participation in the EU-U.S. Privacy Shield.

Moreover, several companies settled with the FTC after they allegedly deceived customers by falsely claiming that they were participants in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system. These include a hand-held vaporizer company, Very Incognito Technologies, enterprise software provider Sentinel Labs, private messaging app marketer SpyChatter, and cybersecurity software distributor Vir2us.

The inferred FTC's standards around making false claims about participating in international privacy agreements:
The implied standard in this category is clear: Companies must not misrepresent their participation, membership, or certification in any privacy or security program sponsored by a government or self-regulatory organization.

Engaging in deceptive privacy-related practices

This category of cases involved companies engaged in alleged misrepresentations of the collection, use, or sale of consumers' information. Expand, which also did business as Gigats, Education Match, and SoftRock, allegedly claimed it was pre-screening job applicants for employers seeking to hire people when it was actually collecting consumer contacts and other information to sell "leads" to post-secondary schools and career training programs. The settlement stipulated a payment by Expand of more than $90 million in equitable relief (suspended on payment of $360,000, due to Expand's ability to pay).

Another lead-generation business, Blue Global, settled with the FTC over a complaint that it misled consumers into filling out loan applications and then sold this sensitive information "to virtually anyone willing to pay for the leads." Although Blue Global represented to consumers that it would find them low-interest rate loans, match them with a lender selected from a network of 100 lenders, that they would be "very likely" to receive a loan after completing its online application, and that the information they provided would be "safe and secure," the company sold the information it collected to entities "without regard to loan terms, whether or not the entity was a lender, or whether the other entity secured the application data in any fashion." The settlement order imposed a suspended monetary judgement of more than $104 million. Turn, Inc. settled with FTC over the complaint that it allegedly deceived customers by continuing to track them even after they had opted out of tracking.

The inferred FTC's standards around deceptive privacy-related practices:
Based on the settlement order that Expand and Blue Global agreed to with the FTC, companies should not:

- Misrepresent their services.
- Transfer sensitive personal information without express informed consent.
- Transfer covered information without mandatory disclosures.

Based on the final consent order agreed to by Turn, companies that track consumers for use in targeted advertising should provide on their websites "a clear and conspicuous disclosure that explains what information is collected and used for" this purpose. All companies should also honor consumers' choices regarding their privacy controls.

Conclusion

Collecting and disclosing consumers' information without providing notice and/or receiving consent was the most common reason for FTC enforcement. All companies should, prior to collecting or disclosing any personal or sensitive information, "clearly and conspicuously disclose to the consumer, separate and apart from any 'privacy policy,' 'terms of use' page, or similar document," the categories of information they collect, use, or share; the identity of any third parties to whom they disclose that information; and all purposes for the collection, use, or sharing of the information, and obtain consumers' "affirmative express consent" to do so.

Multiple complaints also focused on companies that collected information from children under 13 but failed to provide notice to or obtain consent from a parent. To avoid violating the COPPA Rule, companies should take the following actions: provide "direct notice" about the collection and use of children's data to parents, post a "prominent and clearly labeled link" to their information practices on their homepage and each area where they collect personal information from children, obtain "verifiable parental consent" prior to collecting or using any children's information, and protect the "confidentiality, security, and integrity" of children's personal information.

Many settlements also mandated the creation of a comprehensive data security or privacy program, which included conducting risk assessments. In addition to implementing security or privacy programs and conducting risk assessments, companies should obtain an assessment of their programs from a third party. The FTC's settlements with Cornerstone and Company, Bayview Solutions, Wyndham, ASUSTeK, Ruby, TaxSlayer, Uber, Lenovo, VTech, and BLU Products (as well as its final order for LabMD) required these companies not only to implement a comprehensive information security program, but also to have that program assessed by a "qualified, objective, independent third-party professional." Based on what the FTC has required in its settlement orders, such assessments should at a minimum do the following:

- Specify the administrative, technical, and physical safeguards implemented.
- Explain how such safeguards are appropriate to the company's "size and complexity," "the nature and scope of its activities," and "the sensitivity of the personal information collected."

- Certify that the program is operating with "sufficient effectiveness" so that that the security, confidentiality, and integrity of personal information is protected.

This study aimed to decipher the FTC's privacy and data security standards through an analysis of the complaints it has filed and settlements it has reached over the past several years with companies that have been the targets of its Section 5 enforcement authority. Articulating the requirements of these various settlements provides deeper insight into what the FTC expects of companies and what practices it will enforce against. The conclusions of this study can promote a better understanding of what companies should and should not do to comply with U.S. privacy laws and regulations as enforced by the FTC.