Privacy + Security Forum, Fall Academy

Suggested Reading Materials for

Assuring Technical Privacy Compliance: The Best Defense Is a Good Defense

September 30, 2021

1. Federal Trade Commission, *FTC's Use of Its Authorities to Protect Consumer Privacy and Security,* Jun. 18, 2020.
2. Complaint, *In the Matter of Everalbum, Inc.*, May 6, 2021.
3. Decision and Order, *In the Matter of Everalbum, Inc.*, May 6, 2021.
4. Settlement, *In the Matter of App Annie Inc. and Bertrand Schmitt,* Sep. 14, 2021.
5. Latham & Watkins, *FTC Chair Rebecca Slaughter Outlines Data Privacy Enforcement Agenda,* Feb. 12, 2021.
6. Atteberry, Jeffrey; Rubin, Noah; and Wachs, Heidi; *Understanding HIPAA's security rule for telemedicine apps*, Dec. 1, 2020.

FTC's Use of Its Authorities to Protect Consumer Privacy and Security

Federal Trade Commission
2020

FTC Use of its Authorities to Protect Consumer Privacy and Security

This report responds to Senate Appropriations Committee Report 116-111 accompanying the Financial Services and General Government Appropriations Bill, 2020, directing the Federal Trade Commission ("Commission" or "FTC") to report on "the ways it utilizes its current authorities, including Section 5 unfairness authority, to deter unfair and deceptive conduct in consumer privacy and data security matters."

Since the enactment of the Fair Credit Reporting Act ("FCRA")[1] in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy. With the development of the internet as a commercial medium in the 1990s, the FTC expanded its focus on privacy to reflect the growing collection, use, and sharing of consumer data in the commercial marketplace.

Since the enactment of the Fair Credit Reporting Act ("FCRA") in 1970, the FTC has served as the chief federal agency charged with protecting consumer privacy.

As you have requested, we will start by outlining our authority under the FTC Act and Section 5 in particular. We will then discuss some of our other work to deter unfair and deceptive conduct in privacy and data security matters. We will conclude by discussing challenges and limitations of this authority.

I. The FTC Act

Section 5 of the FTC Act prohibits deceptive or unfair commercial practices.[2] Under Section 5, the FTC has aggressively pursued privacy and data security cases in myriad areas, including against social media companies, mobile app developers, data brokers, ad tech industry participants, retailers, and companies in the Internet of Things space.

---

[1] 15 U.S.C. § 1681. Among other things, the FCRA prohibits the unauthorized disclosure of sensitive data used for credit, employment, and other decisions.

[2] 15 U.S.C. § 45. As discussed further below, the Commission also enforces specific statutes containing privacy and data security provisions, such as the Gramm-Leach-Bliley Act ("GLB Act"), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506; the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, which gives effect to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101 et seq.; the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act, 15 USC §§ 7701-7713; and the Fair Credit Reporting Act, 15 U.S.C. § 1681.

To date, the Commission has brought more than 70 cases alleging that companies failed to implement reasonable data security safeguards, and more than 80 general privacy cases.

In order to prove a privacy or security allegation under Section 5, we must show that a company's conduct is "deceptive" or "unfair."

In order to prove a privacy or security allegation under Section 5, we must show that a company's conduct is "deceptive" or "unfair." A representation, omission, or practice is deceptive if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers – that is, it would likely affect the consumer's conduct or decisions with regard to a product or service.[3] We have challenged deceptive claims about privacy and security that appear in privacy policies, user interfaces, FAQ pages, company websites, and product packaging. We have challenged claims about what information a company collects, how it uses the information, how long it keeps the information, who it shares the information with, the ability of consumers to exercise choices with respect to the information, and the level of security provided for the information.

Notably, some deception cases involve omission of material information, the disclosure of which is necessary to prevent the claim, practice, or sale from being misleading. Thus, for example, we have alleged that a company's statement that it is collecting "browsing information" is deceptive, where it fails to tell the consumer that it also collected contents of people's shopping carts, information entered onto banking pages, and search information.[4]

A practice is unfair if (1) it causes or is likely to cause substantial injury (2) the injury is not reasonably avoidable by consumers and (3) the injury is not outweighed by benefits to consumers or competition.[5] We have alleged that several privacy-related practices are unfair, including the following:

---

[3] *See* FTC Policy Statement on Deception (Oct. 23, 1984) (appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 183 (1984)), https://www.ftc.gov/public-statements/1983/10/ftc-policystatement-deception.

[4] *See* FTC Press Release, *Membership Reward Service Upromise Penalized for Violating FTC Order* (Mar. 17, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/membership-reward-service-upromise-penalized-violating-ftc-order; FTC Press Release, *Sears Settles FTC Charges Regarding Tracking Software* (June 4, 2009), https://www.ftc.gov/news-events/press-releases/2009/06/sears-settles-ftc-charges-regarding-tracking-software.

[5] 15 U.S.C. § 45(n).

- Failing to reasonably secure personal information, including financial and health information, and contents of communications.[6]
- Engaging in telephone records pretexting, in which information brokers obtain consumers' phone records under false pretenses (e.g., posing as a customer of a telephone carrier) and sell the information to third parties.[7]
- Soliciting "revenge porn," in which companies solicit intimate pictures and videos of ex-partners, along with their personal information, without their knowledge or consent.[8]
- Developing and marketing "stalkerware," in which purchasers surreptitiously install monitoring software on their partners' phones without their knowledge or consent. The software often tracks geolocation, app usage, and contents of text messages and other communications.[9]
- Activating webcams surreptitiously in leased computers placed in consumers' homes.[10]
- Selling sensitive data such as Social Security numbers to third parties that did not have a legitimate business need for the information, including known fraudsters.[11]

---

[6] *See, e.g.*, In the Matter of InfoTrax Systems, L.C., FTC File No. 162 3130, Docket No. C-4696 (2019); FTC v. Equifax, Civ. Action No. 1:19-cv-03297-TWT (N.D. Ga. 2019); In the Matter of LightYear Dealer Technologies, LLC, d/b/a DealerBuilt, FTC File No. 172 3051, Docket No. C-4687 (2019); In the Matter of James V. Grago, Jr. and d/b/a ClixSense.com, FTC File No. 172 3003, Docket No. C-4678 (2019); United States of America v. Mortgage Solutions FCS, Inc., d/b/a Mount Diablo Lending, Civil Action No. 4:20-cv-00110 (N.D. Cal. 2019); In the Matter of Lenovo, Inc., FTC File No. 152 3134, Docket No. C-4636 (2017); In the Matter of ASUSTeK Computer Inc., FTC File No. 142 3156, Docket No. C-4587 (2016); In the Matter of LabMD, Inc., FTC File No: 102 3099; Docket No. C-9357, Civil Action No. 16-16270 (11th Cir. 2015); In the Matter of Accretive Health, Inc., FTC File No. 122 3077, Docket No. C-4432 (2013); In the Matter of TRENDnet, Inc., FTC File No. 122 3090, Docket No. C-4426 (2013); In the Matter of HTC America, Inc., FTC File No. 122 3049, Docket No. C-4406 (2013); In the Matter of Compete, Inc., FTC File No. 102 3155 (2012); In the Matter of EPN, Inc., also d/b/a as Checknet, Inc., FTC File No. 112 3143, Docket No. C-4370 (2012); US v. Direct Lending Source, Inc., Bailey & Associates Advertising, Inc., Virtual Lending Source, LLC, FTC File No. 102 3000, Civil Action No. 12-CV-2441-DMS-BLM (S.D. Cal. 2012); FTC v. Wyndham Worldwide Corp., Wyndham Hotel Group, LLC, Wyndham Hotels & Resorts, LLC, and Wyndham Hotel Management, Inc., Civil Action No. 2:12-cv-01265-SPL (D.N.J. 2012).

[7] See FTC v. Accusearch, Inc., Case No. 08-8003 (10th Cir. 2009).

[8] *See* FTC and State of Nevada v. EMP Media, Inc. (d/b/a MyEx.com), Civil Action No. 2:18-cv-00035 (D. Nev. 2018); In the Matter of Craig Brittain, FTC File No. 132 3120 Docket No. C-4564 (2015).

[9] *See* In the Matter of Retina-X Studios, LLC, FTC File No. 172 3118 (2019).

[10] In the Matter of DesignerWare, LLC, Docket No. C-4390 (F.T.C. Apr. 15, 2013); In the Matter of Aaron's, Inc., FTC File No. 122 3256 (2013).

[11] FTC v. Sitesearch Corp., d/b/a LeapLab; LeapLab, LLC; Leads Company, LLC, FTC File No. 142 3192, Case No. 2:14-cv-02750 (D. Ariz. Feb. 18, 2016); FTC v. Sequoia One, LLC, Case No. 2:15-cv-01512-JCM-CWH (D. Nev. Nov. 2, 2016); FTC v. Blue Global, LLC, Case No. 2:17-cv-02117-ESW (D. Ariz. July 5, 2017).

- Collecting and sharing sensitive television-viewing information without notice or consent.[12]
- Where a company does not make a deceptive representation or omission, and we cannot prove the three prongs of unfairness, we cannot bring a Section 5 case.[13]

In terms of remedies under Section 5, our orders in these cases include, 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/or requirements to improve transparency and choice mechanisms for consumers. The FTC generally cannot seek civil penalties for initial violations of the FTC Act, but if a company violates an FTC order, the FTC can seek civil monetary penalties for the violations, as it did last year when it announced a $5 billion settlement with Facebook.[14]

The Commission recognizes that achieving effective remedies is a dynamic process that involves continual review of what has been working and what needs further adjustment or strengthening. Thus, from time to time, the Commission has revised standard provisions in orders in order to improve their effectiveness. For example, last year, the Commission worked to strengthen data security orders to require board-level oversight of data security issues where appropriate, set forth more specific requirements (e.g., requirements to encrypt data, segment networks), and improve the accountability of third-party data security assessors.[15]

The FTC can seek civil monetary penalties for the violations, as it did last year when it announced a $5 billion settlement with Facebook.

[12] FTC v. Vizio, Inc., 2:17-cv-00758 (D.N.J. 2017).

[13] The FTC continues to examine new and emerging technology areas, such as biometrics, artificial intelligence, ed tech, and voice-activated devices.

[14] *See* FTC Press Release, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[15] The appellate court decision in *LabMD* also was part of the impetus for the Commission to re-evaluate the data security provisions in its orders. In that decision, the court found, *inter alia*, that the requirement to "establish, implement, and maintain a reasonable data security program" was unenforceable because of lack of specificity. *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221, 1237 (11th Cir. 2018). The result in that case underscores the challenges the Commission faces when litigating violations of Section 5 of the FTC Act stemming from data security practices and the need for federal data security legislation.

The FTC Act also authorizes the Commission to promulgate trade regulation rules to address prevalent unfair or deceptive practices, and to seek civil penalties against those who violate them with actual knowledge or with knowledge fairly implied.[16] Section 18 of the FTC Act, 15 U.S.C. § 57a, added by the Magnuson-Moss Warranty—FTC Improvements Act, Pub. L. No. 93-637 (1975), establishes a set of procedures that the FTC must follow in promulgating these rules. These procedures include the following: (1) publication of an advance notice of proposed rulemaking ("ANPR"), an opportunity for public comment on the ANPR, and a determination by the Commission, before issuing a notice of proposed rulemaking, that the acts or practices at issue are "prevalent;" (2) submission of both the ANPR and the NPR to Congressional oversight committees; (3) a mandatory oral hearing, if any person requests one, presided over by an independent hearing officer; (4) preparation of a staff report and recommendations to the Commission on the rulemaking record; (5) submission of the hearing officer's recommended decision to the Commission; (6) a public comment period; (7) special judicial review provisions that allow parties to apply to the court for leave to make additional oral submissions or written presentations. Even under the best of circumstances, this would be a lengthy process.[17] For a variety of reasons, the Commission has not engaged in this type of rulemaking on privacy and security.

II. Other Authority

In addition to the FTC Act, the FTC has authority to enforce a variety of specific laws in the privacy area, including the Gramm-Leach-Bliley Act ("GLB"), which protects the privacy of financial information; the CAN-SPAM Act, which allows consumers to opt out of receiving commercial email messages; the Children's Online Privacy Protection Act ("COPPA"); the Fair Credit Reporting Act ("FCRA"), which protects the privacy of consumer report information; the Fair Debt Collection Practices Act, which protects consumers from harassment by debt collectors; and the Telemarketing and Consumer Fraud and Abuse Prevention Act, under which the FTC implemented the Do Not Call registry.[18] The FTC has brought

The FTC has brought more than 100 cases against companies for violating the FCRA, and close to 30 COPPA cases.

[16] 15 U.S.C. § 57a.

[17] *See* 15 U.S.C. §§ 57a & § 57b-3; 16 C.F.R. § 1.13.

[18] *See* Gramm-Leach-Bliley Act ("GLB Act"), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.); Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), 15 U.S.C. §§ 7701-7713; Children's Online Privacy

more than 100 cases against companies for violating the FCRA, and close to 30 COPPA cases. Since 2003, the FTC has brought 147 cases enforcing Do Not Call provisions against telemarketers, and more than 130 spam and spyware cases. Since 2005, the FTC has brought about 35 cases alleging violations of the GLB Act and its implementing regulations. The Commission has used these authorities to take action against large, well-known companies such as YouTube and Equifax, as well as smaller companies that we allege to have engaged in illegal practices, such as, most recently, a mortgage company that retaliated against consumers by disclosing consumers' credit information on Yelp, in violation of the Fair Credit Reporting Act and other statutes.[19] In contrast to Section 5, many of these statutes allow us to seek civil penalties for first time violations.

In addition to our enforcement efforts on privacy and data security, the Commission seeks to improve agency decision-making through its policy initiatives. Since 2010, we have conducted 45 workshops on privacy issues and issued 29 reports. For example, over the past 18 months, the Commission held four days of hearings that specifically addressed consumer privacy and data security.[20] The Commission also announced its fifth PrivacyCon, which will take place on July 21, 2020, an annual event that explores evolving privacy and data security research.[21] Finally, the Commission is empowered to conduct industry studies related to privacy and data security under Section 6(b) of the FTC Act.[22] Last year, we issued 6(b) orders to several internet service providers to

---

Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506; Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681; Fair Debt Collection Practices Act ("FDCPA"), 15 U.S.C. § 1692; Telemarketing and Consumer Fraud Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108.

[19] *See* FTC Press Release, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law* (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations; FTC Press Release, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related; FTC Press Release, *Mortgage Broker That Posted Personal Information about Consumers in Response to Negative Yelp Reviews Settles FTC Allegations* (Jan. 7, 2020), https://www.ftc.gov/news-events/press-releases/2020/01/mortgage-broker-posted-personal-information-about-consumers.

[20] *See* FTC Press Release, *FTC Announces Sessions on Consumer Privacy and Data Security as Part of Its Hearings on Competition and Consumer Protection in the 21st Century* (Oct. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-announces-sessions-consumer-privacy-data-security-part-its.

[21] *See* FTC Press Release, *FTC Announces PrivacyCon 2020 and Calls for Presentations* (Oct. 11, 2019), https://www.ftc.gov/news-events/press-releases/2019/10/ftc-announces-privacycon-2020-calls-research-presentations.

[22] 15 U.S.C. § 46(b).

report on their privacy practices.[23] As we have in the past, we will use the information we learn from this study to better inform our policy and enforcement work.

In all of our privacy and data security work, the FTC's goals have remained constant: to protect consumers' personal information and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace. The attached Appendix provides additional details about how we have used our existing authority. Appendix A (Federal Trade Commission 2019 Privacy and Data Security Update).

III. Challenges and Limitations

Section 5 does not generally allow the Commission to seek civil penalties for a first-time offense.

Despite our use of these authorities, we face several limitations and challenges. First, Section 5 does not generally allow the Commission to seek civil penalties for a first-time offense. Relatedly, because our Section 5 authority relies heavily on individual case enforcement and judicial interpretation, adverse decisions can have an outsized effect on our enforcement ability. For example, recent decisions questioning our ability to obtain injunctive and monetary relief have allowed opposing parties to challenge the agency's pursuit of that relief,[24] presenting further hurdles in obtaining monetary relief for consumers in this area.[25]

Second, while we have Administrative Procedure Act ("APA") rulemaking authority for specific statutes (like COPPA), we do not have APA rulemaking authority generally, which limits how quickly rules can be made. While the Commission possesses Magnuson-Moss rulemaking authority under Section 18 as discussed above, targeted authority to enact

---

[23] *See* FTC Press Release, *FTC Seeks to Examine the Privacy Practices of Broadband Providers* (Mar. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-examine-privacy-practices-broadband-providers.

[24] *See, e.g., FTC v. Zurixx, LLC*, 2020 WL 927531 (D. Utah Feb. 26, 2020); *FTC v. Simple Health Plans, LLC*, 2020 WL 570811 (11th Cir. Feb. 5, 2020); *FTC v. Nudge*, 2019 WL 7398678 (D. Utah Dec. 31, 2019); *FTC v. AMG Capital Mgmt.*, LLC, 910 F.3d 417 (9th Cir. Dec. 3, 2018), *petition for cert. filed* (U.S. Oct. 18, 2019).

[25] *F.T.C. v. Credit Bureau Center, LLC*, 937 F.3d 764, 767 (7th Cir. 2019) (holding section 13(b) does not authorize restitutionary relief, and overruling *FTC v. Amy Travel Service, Inc.*, 875 F.2d 564 (7th Cir. 1989)); *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221, 1237 (11th Cir. 2018) (holding that FTC order was unenforceable because of lack of specificity); and *Kokesh v. S.E.C.*, 137 S.Ct. 1635, 1639 (2017) (holding disgorgement in the securities-enforcement context is a "penalty" within the meaning of a securities statute similar to Section 5, so disgorgement actions must be commenced within five years of the date the claim accrues).

privacy rules under the APA would better allow us to ensure that the law keeps up with changes in technology. As noted above, Magnuson-Moss rulemaking authority is a more complex process that requires additional procedural hurdles and historically has taken significantly longer than rulemakings that proceed under the APA, rendering it an imperfect tool for the rapidly evolving space of data privacy.[26] *See* 15 U.S.C. § 57a. Where Congress has given us APA rulemaking authority, we have used it. For example, Congress enacted COPPA in 1998, at a time when children were not using mobile devices or uploading photos on social media sites. In 2012, the Commission used its APA rulemaking authority to expand the parental consent required under COPPA to photos and videos uploaded by children, and to apply the statute to the collection of persistent identifiers, like IP addresses. It also clarified that the collection of geolocation information would trigger COPPA's requirements.

Third, Section 5 excludes non-profits and common carriers from the Commission's authority, even when the acts or practices of these market participants have serious implications for consumer privacy and data security. Indeed, many data breaches over the years have taken place in the non-profit educational sector.

For these reasons, to better equip the Commission to meet its statutory mission to protect consumers, we urge Congress to enact privacy and data security legislation, enforceable by the FTC, which grants the agency civil penalty authority, targeted APA rulemaking authority, and jurisdiction over non-profits and common carriers.[27, 28]

---

[26] Specifically, to propose a Mag-Moss rule, the Commission will be required to, among other things, publish an Advance Notice of Proposed Rulemaking with a 30-day public comment period, provide an opportunity for public hearings, publish a staff report, receive and review a presiding officer report on any hearings, and hold a 60-day public comment period on the staff and presiding officer reports. 15 U.S.C. § 57a; 16 C.F.R. § 1.13.

[27] Commissioner Phillips supports congressional efforts to consider consumer data privacy legislation. He believes legislation should be based on harms that Congress agrees warrant a remedy, and that tools like penalties and rulemaking should be calibrated carefully to address those harms. Commissioner Phillips believes Congress should also give appropriate consideration to the trade-offs involved in new regulation, and, with regard to rulemaking, reserve to itself fundamental value judgments appropriately made by the legislature. Finally, Commissioner Phillips believes data security legislation is a critical step Congress should also take to protect consumer privacy.

[28] *See also* Concurring Statement of Commissioner Rohit Chopra, *Issuance of Federal Trade Commission Report, FTC's Use of Its Authorities to Protect Consumer Privacy and Security* (June 18, 2020), available at https://www.ftc.gov/public-statements/2020/06/statement-commissioner-rohit-chopra-regarding-report-congress-ftcs-use-its.

Appendix: Federal Trade Commission 2019 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 Gramm-Leach-Bliley Act, the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (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. The Commission has used its authority 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 Promote Data Security?

The FTC uses every tool at its disposal 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 steps to remediate the unlawful behavior. This has included, 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 providing robust transparency 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, the Telemarketing Sales Rule, the Fair Debt Collection Practices Act, and the CAN-SPAM Act.

The FTC uses every tool at its disposal 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 steps to remediate the unlawful behavior.

Using its existing authority, the Commission has brought hundreds of privacy and data security cases to date. To better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested

[1] This document covers the time period from January 2019-December 2019. It will be re-issued on an annual basis.

legislation would expand the agency's civil penalty authority, provide the agency with targeted rulemaking authority, and extend the agency's commercial sector jurisdiction to non-profits and common carriers as well.

Beyond enforcement, the FTC's 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.

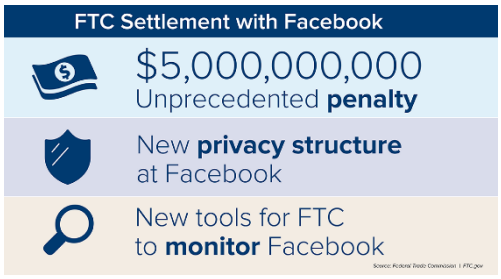
In all of its privacy and data security work, the FTC's goals have remained constant: to protect consumers' personal information; and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace.

ENFORCEMENT

The FTC, building on decades of experience in consumer privacy enforcement, continued in 2019 to conduct investigations and bring cases addressing practices offline, online, and in the mobile environment, as described below. The FTC's cases generally focus on protecting American consumers, but in some cases also protect foreign consumers from unfair or deceptive practices by businesses subject to the FTC's jurisdiction.

General Privacy

The FTC has brought enforcement actions addressing a wide range of privacy issues in a variety of industries, including social media, ad tech, and the mobile app ecosystem. These matters include **more than 130 spam and spyware cases** and **80 general privacy lawsuits**. In 2019, the FTC announced the following privacy cases:



- On July 24, 2019, the Commission and the U.S. Department of Justice announced a settlement with Facebook. The complaint alleged that Facebook violated the Commission's 2012 order against the company by misrepresenting the control users had over their personal information, and failing to institute and maintain a reasonable program to ensure consumers' privacy. It also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users. The Facebook order imposed a $5 billion penalty, as well as a host of modifications to the Commission's order designed to change Facebook's overall approach to privacy. The $5 billion penalty against Facebook is the largest ever imposed on

any company for violating consumers' privacy. The settlement is currently pending approval by the United States District Court for the District of Columbia.

- In a related, but separate case, the FTC also filed a law enforcement action against the data analytics company Cambridge Analytica, as well as its former Chief Executive Officer, Alexander Nix, and app developer, Aleksandr Kogan. The FTC's complaint alleged that Cambridge Analytica, Nix, and Kogan used false and deceptive tactics to harvest personal information from millions of Facebook users for voter profiling and targeting. The complaint alleged that app users were falsely told the app would not collect users' names or other identifiable information. Contrary to this claim, the complaint alleged, the app collected users' Facebook User ID, which connects individuals to their Facebook profiles. Kogan and Nix agreed to settlements with the FTC that restrict how they conduct any business in the future, and the Commission entered a default judgment against Cambridge Analytica. The Commission's opinion holds that Cambridge Analytica violated the FTC Act through the deceptive conduct and reaffirms the proposition that, like any other claim, a company's privacy promises are viewed through the lens of established FTC consumer protection principles.

- The FTC brought its first action against a developer of stalking apps—software that allows purchasers to monitor the mobile devices on which they are installed, without users' knowledge. In its complaint, the FTC alleged, among other things, that Retina-X sold apps that required circumventing certain security protections implemented by the mobile device operating system or manufacturer, and did so without taking reasonable steps to ensure that the apps would be used only for legitimate and lawful purposes. The complaint alleged that the company's practices enabled use of its apps for stalking and other illegitimate purposes. The proposed order requires the company and its owner to refrain from selling products or services that monitor devices, without taking steps to ensure that the products or services will be used for legitimate purposes.

- Unrollme, Inc., an email management company, settled allegations that it deceived consumers about how it accesses and uses their personal emails. According to the complaint, Unrollme falsely told consumers that it would not "touch" their personal emails in order to persuade consumers to provide access to their email accounts. In fact, the complaint alleged, Unrollme was sharing the consumers' email receipts—which can include, among other things, the user's name, billing and shipping addresses, and information about products or services purchased by the consumer—with its parent company, Slice Technologies, Inc. According to the complaint, Slice used anonymous purchase information from Unrollme users' e-receipts in the market research analytics products it sells. As part of the settlement with the Commission, Unrollme is prohibited from misrepresenting the extent to which it collects, uses, stores, or shares

information from consumers. It is also required to notify consumers and delete the data unlawfully collected from consumers, unless it obtains their affirmative, express consent to maintain the e-receipts.

- In Effen Ads, LLC (iCloudWorx), the FTC obtained stipulated final orders against defendants that promoted a work-from-home program through unsolicited email, or spam, claiming that consumers could make significant income with little effort. The spam emails included misleading "from" lines and links to websites that falsely claimed that various news sources had favorably reviewed the program, and "subject" lines that displayed false celebrity endorsements. The stipulated final orders permanently ban defendants from marketing or selling either work-from-home programs or business opportunities or business coaching products, and permanently enjoined them from violating the CAN-SPAM Act. The orders also impose judgments totaling more than $12.6 million, and require defendants to pay nearly $1.5 million in partial satisfaction of the judgments.

- In Global Asset Financial Services Group, LLC, the FTC shut down a phantom debt brokering and collection scheme. The Commission charged the defendants with purchasing and collecting on counterfeit debts fabricated from misappropriated information about consumers' identities as well as finances and debts purportedly owed on bogus "autofunded" payday loans. In numerous instances, defendants also disclosed consumers' purported debts to third parties. The final orders, imposing a combined judgment of more than $13 million, ban all the defendants from the debt collection business and from misleading consumers about debt. They also prohibit defendants from profiting from customers' personal information collected as part of the challenged practices, and failing to dispose of such information properly.

- In Hylan Asset Management, LLC, the FTC and the New York Attorney General's Office charged two operations—Hylan Asset Management, LLC and its related companies (Hylan) and Worldwide Processing Group, LLC (Worldwide)—as well as their principals with buying, placing for collection, and selling lists of phantom debts, including debts that were fabricated by the defendants or disputed by consumers. The Commission alleged that the defendants obtained consumers' private financial information and then used it to convince consumers they were legitimate collectors calling about legitimate debts. The FTC also alleged that, in numerous instances, the Worldwide defendants unlawfully communicated with third parties where they already possessed contact information for the consumer. The FTC secured final orders banning the Hylan defendants from the debt collection industry and prohibiting the Worldwide defendants from unlawful debt collection practices. The orders prohibit all defendants from using customers' personal information and failing to properly dispose of that information.

- In ACDI Group, the Commission charged the defendants with collecting on a portfolio of counterfeit payday loan debts, which included financial information, such as Social Security and bank account numbers. When the defendants reported to the debt broker who had sold them the portfolio that they had

received consumer complaints regarding the legitimacy of the debts, the broker returned the defendants' money and told them to stop collecting; however, the defendants allegedly continued to do so for at least seven more months. The final order, entered in December 2019, requires the defendants to provide full redress to injured consumers and prohibits the defendants from disclosing, using, or benefitting from previously obtained consumer information that is unverified.

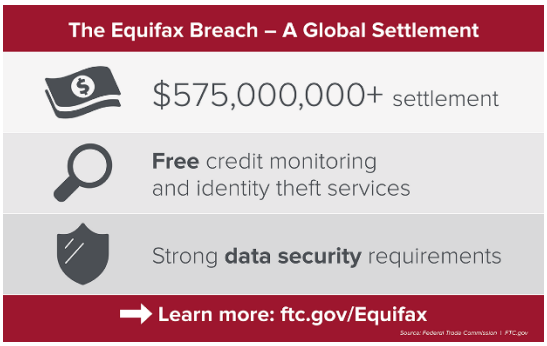
- In Grand Teton Professionals LLC, the FTC charged defendants with running a credit repair scheme that collected more than $6.2 million in illegal upfront fees and falsely claimed to repair consumers' credit. Among other things, the Commission alleged that the operation obtained sensitive consumer data, like Social Security numbers and dates of birth, for bogus credit repair services.

- In Mission Hills Federal, the FTC obtained a temporary restraining order halting a student loan debt relief scheme. The defendants promised student loan assistance and allegedly then used consumer's personal information to effectively assume consumers' identities with their federal loan servicers. According to the FTC's filings, the defendants did this to prevent consumers from learning the defendants were actually pocketing millions of dollars in consumers' student loan payments instead of paying down their loans or providing debt relief.

- In Career Education Corporation, the FTC obtained stipulated final orders against defendants that used deceptive lead generators to market their schools. The defendants' lead generators used deceptive tactics, such as posing as military recruiting websites, to induce consumers to provide their information online. Those websites promised consumers that the information submitted would not be shared with anyone else, but the lead generators sold that information to the defendants to market their schools. The stipulated final order imposes a $30 million judgment for consumer redress, and requires defendants to launch a system to review the materials that lead generators use to market their schools, to investigate complaints about lead generators, and to not use or purchase leads obtained deceptively or in violation of the Telemarketing Sales Rule.

Data Security and Identity Theft

Since 2002, the FTC has brought **more than 70 cases** against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. In 2019, the FTC strengthened its standard orders in data security cases. Each of the cases discussed below resulted in settlements that, among other things, required the companies to implement a comprehensive security program, obtain robust biennial assessments of the program, and submit annual certifications by a senior officer about the company's compliance with the order.



- The FTC's complaint against Equifax alleged that the company failed to secure the massive amount of personal information stored on its network. Among other things, the company allegedly failed to patch well-known software vulnerabilities, failed to segment its database servers, and stored Social Security numbers in unencrypted, plain text. According to the complaint, these failures led to a breach that affected more than 147 million people, and exposed millions of names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud. The settlement, which totals between $575 million and $700 million, was part of a global resolution where Equifax settled matters with a consumer class action, the Consumer Financial Protection Bureau, and 50 states and territories.

- In July, the FTC announced a complaint and settlement against the operator of ClixSense.com, an online rewards website that pays its users to view advertisements, perform online tasks, and complete online surveys. The complaint alleged that the website's operator, James V. Grago, Jr., deceived consumers by falsely claiming that ClixSense "utilizes the latest security and encryption techniques to ensure the security of your account information." In fact, ClixSense failed to implement minimal data security measures and stored personal information—including Social Security numbers—in clear text with no encryption, according to the complaint. The FTC alleged that ClixSense's failures allowed hackers to gain access to the company's network, resulting in a breach of 6.6 million consumers' information.

- The FTC settled charges against Unixiz, d/b/a i-Dressup.com, a dress-up games website, alleging that the company and its owners stored and transmitted users' personal information in plain text and failed to perform vulnerability testing of its network, implement an intrusion detection and prevention system, and monitor for potential security incidents. These failures led to a security breach in which a hacker accessed the information of approximately 2.1 million users—including approximately 245,000 users who indicated they were under 13.

- As discussed above, the FTC alleged that Retina-X, a company that sold so-called "stalking apps," and its owner claimed that "Your private information is safe with us." Despite this claim, the company and its owner failed to adopt and implement reasonable information security policies and procedures.

- In its complaint against a provider of software to help auto dealers with management of their inventory, personnel, and customers, the FTC alleged that LightYear Dealer Technologies, LLC, d/b/a DealerBuilt failed to implement readily available and low-cost measures to protect the personal information it collected. These failures led to a data breach in which a hacker gained access to the

unencrypted personal information—such as Social Security numbers and other sensitive data—of about 12.5 million consumers.

- The FTC settled charges against InfoTrax Systems, a technology company that provides back-end operation services to multi-level marketers. The FTC alleged that a hacker infiltrated InfoTrax's server, along with websites maintained by the company on behalf of clients, more than 20 times and accessed the personal information of more than a million consumers. According to the complaint, InfoTrax and its former CEO, Mark Rawlins, failed to use reasonable, low-cost, and readily available security protections to safeguard the personal information they maintained on behalf of their clients.

- Smart home products manufacturer D-Link Systems, Inc. agreed to implement a comprehensive software security program in order to settle FTC allegations over misrepresentations that the company took reasonable steps to secure its wireless routers and Internet-connected cameras. The settlement ended FTC litigation against D-Link stemming from a 2017 complaint in which the agency alleged that, despite claims touting device security, vulnerabilities in the company's routers and Internet-connected cameras left sensitive consumer information, including live video and audio feeds, exposed to third parties and vulnerable to hackers.

Credit Reporting & Financial Privacy

The Fair Credit Reporting Act (FCRA) sets out requirements for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has brought **more than 100 cases** against companies for violating the FCRA and has collected **more than $40 million in civil penalties**. The Gramm-Leach-Bliley (GLB) Act requires financial institutions to send customers initial and 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 about 35 cases alleging violations of the GLB Act and its implementing regulations. In 2019, the FTC brought the following cases:

The FTC has brought more than 100 cases against companies for violating the FCRA and has collected more than $40 million in civil penalties.

- In the Equifax case, discussed above, the FTC alleged that the credit reporting agency violated the GLB Safeguards Rule. Specifically, the complaint alleged that Equifax failed to design and implement safeguards to address foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; regularly test or monitor the effectiveness of the safeguards; and evaluate and adjust its information security program in light of the results of testing and monitoring, and other relevant circumstances.

- In Dealerbuilt, discussed above, the FTC alleged that the company violated the Safeguards Rule by failing to: develop, implement and maintain a written information security program; identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; assess the sufficiency of any safeguards in place to control those risks; and design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures.

International Enforcement

The FTC enforces the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System.

The EU-U.S. Privacy Shield Framework provides a legal mechanism for companies to transfer personal data from the European Union to the United States. This Framework, administered by the U.S. Department of Commerce, helps protect consumers' privacy and security through an agreed set of Privacy Shield Principles. The FTC plays a role in enforcing companies' privacy promises under the Framework as violations of Section 5 of the FTC Act. This year, the FTC participated, alongside the U.S. Department of Commerce and other U.S. government agencies, in the third Annual Review of the Framework, which became operational in August 2016. Following the review, the European Commission announced its continued support for the Privacy Shield, pointing to increased FTC enforcement actions as contributing to the effective functioning of the Framework.

The FTC also serves as a privacy enforcement authority in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CPBR) System. The APEC CBPR System is a voluntary, enforceable code of conduct designed to enhance the privacy and security of consumers' personal information transferred among the United States and other APEC members. Under the System, participating companies can be certified as compliant with APEC CBPR program requirements that implement APEC's nine data privacy principles.

Carrying out its enforcement role under these international privacy frameworks, the FTC has brought **64 actions—39 under the previous "U.S.-EU Safe Harbor" program, 4 under APEC CBPR, and 21 under Privacy Shield.**

Carrying out its enforcement role under these international privacy frameworks, the FTC has brought 64 actions—39 under the previous "U.S.-EU Safe Harbor" program, 4 under APEC CBPR, and 21 under Privacy Shield.

During the past year, the FTC brought the following 13 cases:

- In eight separate actions, the FTC charged that 214 Technologies, Click Labs, DCR Workforce, Incentive Services, LotaData, Medable, SecurTest, and Thru falsely claimed participation in Privacy Shield. While the companies initiated Privacy Shield applications with the U.S. Department of Commerce, the companies did not complete the steps necessary to be certified as complying with the Framework. Because they failed to complete certification, they were not certified participants in the Framework, despite representations to the contrary.

- In separate actions, the FTC charged that Empiristat, Global Data Vault, and TDARX falsely claimed participation in Privacy Shield. The companies had allowed their certifications to lapse while still claiming participation. Further, the companies allegedly failed to verify annually that statements about their Privacy Shield practices were accurate, and failed to affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the program.

- As a part of the FTC's action against Cambridge Analytica, described above, the FTC determined that the company falsely claimed to participate in Privacy Shield after allowing its certification to lapse. Among other things, the Final Order prohibits Cambridge Analytica from making misrepresentations about the extent to which it protects the privacy and confidentiality of personal information, as well as its participation in the EU-U.S. Privacy Shield Framework and other similar regulatory or standard-setting organizations.

Children's Privacy

The Children's Online Privacy Protection Act of 1998 ("COPPA") generally requires websites and apps to obtain verifiable parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought close to 30 COPPA cases and collected hundreds of millions of dollars in civil penalties. During the past year, the Commission took the following actions:

- The FTC's settlement with Google and its subsidiary YouTube—brought in conjunction with the New York Attorney General—alleges that the company collected kids' personal data without parental consent, in violation of the COPPA Rule. The complaint alleges that YouTube violated the COPPA Rule by collecting personal information—including in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent. The $170 million judgment represents the largest civil penalty amount under COPPA.

- Musical.ly, now known as TikTok, is the operator of a video social networking app that allows users to create short videos of themselves lip-syncing to music and to share those videos with other users. In 2019, the company paid $5.7 million to settle charges that it violated COPPA by illegally collecting personal information from children. The complaint alleged the app was child-directed, and that many users self-identified as being under 13.

- The FTC's complaint against Unixiz, Inc., d/b/a i-Dressup.com, discussed above, alleged that the company and its principals violated COPPA by failing to obtain verifiable parental consent before collecting personal information from children under 13. To gain access to all the features on the website, including the social networking features, users had to register as members by submitting a user name, password, birthdate, and email address. If a user indicated he or she was under 13, the registration field asked for a parent's consent. If a parent declined to provide consent, the under-13 users were given a "Safe Mode" membership allowing them to login to access i-Dressup's games and features but not its social features. The FTC alleges, however, that i-Dressup still collected personal information from these children, even if their parents did not provide consent.

- In the Retina-X case, discussed above, the FTC alleged that the respondents failed to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Do Not Call

In 2003, the FTC amended the Telemarketing Sales Rule (TSR) to create a national Do Not Call (DNC) Registry, which now includes more than **235 million active registrations**. Do Not Call provisions 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 DNC Registry, calling consumers after they have asked not to be called again, and using robocalls to contact consumers to sell goods or services. Since 2003, the FTC has brought **147 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 490 companies and 393 individuals involved. The 139 cases concluded thus far have resulted in orders totaling over $1.7 billion in civil penalties, redress, or disgorgement, and actual collections exceeding $160 million. During the past year, the Commission initiated actions and settled or obtained judgments as described below:

The FTC has brought **147 cases enforcing Do Not Call Provisions against telemarketers**.

- In the Educare action, the FTC and the Ohio Attorney General obtained temporary restraining orders, preliminary injunctions, and asset freezes against

an enterprise that ran a fraudulent credit card rate reduction scheme, including four individuals and six corporate entities. One defendant is a provider of Voice over Internet Protocol ("VoIP") services that transmitted the illegal robocalls for the enterprise. This marks the FTC's first enforcement action against a VoIP provider. In granting the FTC's preliminary injunction, the court rejected arguments from the defendants challenging the FTC's jurisdiction over provision of VoIP services. As the litigation continues, all of the corporate defendants are under a receivership.

- The FTC obtained a $30 million civil penalty settlement in its case against Career Education Corporation, discussed above, a post-secondary education company that called numbers on the DNC Registry and used deceptively obtained consumer consent.

- In the EduTrek case, the FTC brought claims against some of the deceptive lead generators hired by Career Education Corporation. To lure consumers into providing their contact information through online ads, the defendants used misleading seals of several federal government agencies. The complaint alleges that the defendants made calls to consumers who had submitted their contact information on websites that claim to help them apply for jobs, health insurance, unemployment benefits, Medicaid coverage, or other forms of public assistance. Instead of offering consumers what was promised on the websites, the defendants marketed training and education programs. The defendants allegedly violated the TSR by initiating over five million unsolicited outbound telemarketing calls to numbers on the DNC Registry, and by providing substantial assistance to other telemarketers who placed calls to numbers on the DNC Registry. Litigation continues in this matter.

- The FTC settled claims with Media Mix 365 and its owners, who developed leads for home solar energy companies. Media Mix called millions of phone numbers on the DNC Registry and repeatedly or continuously called consumers with the intent of annoying, abusing, or harassing them. The settlement imposed a $7.6 million civil penalty judgment, to be suspended if the defendants made timely payment of $264,000. The order also permanently bans Media Mix and its owners from violating the TSR.

- In the Bartoli action, the FTC resolved claims against a robocaller who blasted millions of illegal robocalls to numbers on the DNC Registry, often using spoofed caller ID numbers. In the last six months of 2017 alone, the complaint alleges that Bartoli placed more than 57 million calls to phone numbers on the Registry. Bartoli had been a telemarketer for several companies the FTC had sued in prior cases. Under the final order, Bartoli is permanently banned from calling phone numbers listed on the DNC Registry, sending robocalls, and using deceptive caller ID practices, such as spoofing. The order also imposed a $2.1 million civil penalty judgment, which has been suspended based on Bartoli's inability to pay.

- The FTC's case against 8 Figure Dream Lifestyle, Online Entrepreneur Academy, and their owners preliminarily shut down a fraudulent money making scheme that used illegal robocalls to find victims. The defendants made false or unsubstantiated claims about how much consumers could earn through their programs, often falsely claiming that a typical consumer with no prior skills could make $5,000 to $10,000 in 10 to 14 days of buying the program. The FTC obtained a court ordered temporary restraining order and preliminary injunction, together with an asset freeze to preserve funds for potential consumer redress. Litigation continues.

- In First Choice Horizon, the FTC halted a fraudulent credit card interest rate reduction scheme that contacted its victims through illegal robocalls. The defendants targeted seniors and deceptively told consumers that, for a fee, the defendants could lower their interest rates to zero for the life of the debt, thereby saving the consumers thousands of dollars on their credit card debt. The FTC obtained a temporary restraining order and preliminary injunction, including an asset freeze and the appointment of a receiver to operate the corporate defendants. Litigation is ongoing.

- In FTC v. Jasjit Gotra, the FTC won a preliminary injunction against lead defendant Gotra, banning him from outbound telemarketing while the case proceeds in litigation against him. The FTC also settled claims with defendant Alliance Security. Alliance Security is a home security installation company that, directly and through its authorized telemarketers, called millions of consumers whose numbers were on the DNC Registry. In its settlement, Alliance Security agreed to a complete ban on all telemarketing. Thus far, through five settlements in the case, the FTC has obtained judgments totaling more than $14 million.

ADVOCACY

When courts, government agencies, 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 2019, the FTC filed the following comments related to privacy issues:

- The FTC filed a comment on National Institute of Standards and Technology (NIST) proposed privacy framework, which attempts to provide guidance to organizations seeking to manage privacy risks. In the comment, staff of the FTC's Bureau of Consumer Protection commended NIST for proposing a voluntary tool aimed at helping organizations start a dialogue about managing privacy risks within their organizations. The comment suggested certain changes to the proposed framework. For example, it called for greater attention to the need to address the risk of privacy breaches at each step of the Draft Privacy Framework; clarification that procedures for managing privacy risks should account for the sensitivity of the information; and a call for companies to review

whether their actual data practices align with consumer expectations and public-facing statements.

- The FTC testified before Congress numerous times on privacy and data security issues. For example, the Commission called for privacy and data security legislation in testimony before the House and Senate Appropriations Committees and the House Energy and Commerce Committee. The FTC also testified on the need for data security legislation before the Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations and before the House Oversight and Reform Subcommittee on Economic and Consumer Policy.

RULES

Congress has authorized the FTC to issue 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. In 2018, the FTC announced a regulatory review, in which it sought public comment to determine whether it should update the Rule in light of new developments in the marketplace. The public comment period closed in 2019, and the FTC is evaluating next steps.

- The COPPA Rule requires websites and apps to get parental consent before collecting personal information from children under 13. In 2019, as part of its ongoing effort to ensure that its rules are keeping up with emerging technologies and business models, the Commission announced that it was seeking comment on the effectiveness of the 2013 amendments to the COPPA Rule and whether additional changes are needed. The public comment period closed later in 2019, and the FTC is evaluating next steps.

The COPPA Rule requires websites and apps to get parental consent before collecting personal information from children under 13.

- The GLB Privacy Rule sets forth when car dealerships must provide customers with initial and annual notices explaining the dealer'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. In 2019, the FTC issued a Notice of Proposed Rulemaking seeking comments on both the GLB Privacy and Safeguards Rules. The public comment period closed later in 2019, and the FTC is evaluating next steps.

- 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 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. Following a public comment period as part of its systemic review of all current FTC rules and guides, in 2019 the FTC determined that it would confirm the CAN-SPAM Rule without change.

- 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.

- In June 2019, the FTC finalized the Military Credit Monitoring Rule, which requires nationwide consumer reporting agencies to provide free electronic credit monitoring services for active duty military consumers. The final Rule requires the nationwide consumer reporting agencies to notify active duty military consumers within 48 hours of any material additions or modifications to their credit files. The Rule also requires that when a credit reporting agency (CRA) notifies an active duty military consumer about a material change to their credit file, the CRA must also provide that consumer with free access to that file. Further, the Rule contains restrictions on secondary uses and disclosures of information collected from an active duty military consumer requesting the credit monitoring service, and also bans marketing during the enrollment process until after an active duty military consumer has been enrolled in the free credit monitoring service.

WORKSHOPS

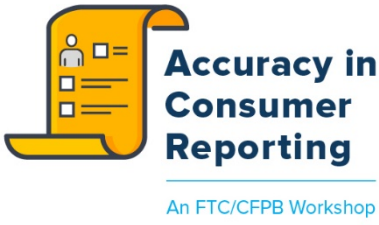
Beginning in 1996, the FTC has hosted **more than 75** workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2019, the FTC hosted the following privacy events:

- In April, as part of the agency's Hearings on Competition and Consumer Protection in the 21st Century, the Commission hosted a hearing on the Commission's authority to deter unfair and deceptive conduct in privacy matters. The FTC's Approach to Consumer Privacy explored topics, such as: the risks and benefits to consumers of information collection, sharing, aggregation, and use; the use of "big data" in automated decisionmaking; how firms that interface directly with consumers foster accountability of third parties to whom they transfer consumer data; and what is the best way to provide consumers with the right balance of information with respect to privacy protections.

- In June, the Commission hosted its fourth annual PrivacyCon, a conference to examine cutting-edge research and trends in protecting consumer privacy and security. The event brought together leading stakeholders, including researchers, academics, industry representatives, federal policymakers, and consumer advocates. PrivacyCon 2019 explored the privacy and security implications of emerging technologies, such as the Internet of Things, artificial intelligence, and virtual reality.

- In October, the Commission hosted a workshop examining whether to update the COPPA Rule in light of evolving business practices in the online children's marketplace, including the increased use of Internet of Things devices, social media, educational technology, and general audience platforms hosting third-party child-directed content.

- In December, the Commission, along with the Consumer Financial Protection Bureau, hosted a workshop on accuracy in consumer reporting. The workshop brought together stakeholders—including industry representatives, consumer advocates, and regulators—for a wide-ranging public discussion on the many issues that affect the accuracy of consumer reports. Panels focused on both the accuracy of both traditional credit reports and employment and tenant background screening reports, particularly in light of changes to the marketplace since 2012.



CONSUMER EDUCATION AND BUSINESS GUIDANCE

The Commission has distributed millions of copies of educational materials, many of which are published in both English and Spanish, and generated millions of online pageviews to help consumers and businesses 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, Do Not Call, and computer security. Examples of such education and guidance materials developed in 2019 include:

- **Cybersecurity for Small Business Campaign.** The FTC continued to promote its Cybersecurity for Small Business campaign, created with the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Small Business Administration (SBA). In 2019, the agency released campaign materials in Spanish covering a dozen topics, including cybersecurity basics, understanding the NIST Cybersecurity Framework, and vendor security. Outreach in 2019 included webinars to state Small Business Development Centers, a social media campaign, regional events for National Small Business Week, a ransomware webinar for Texas municipalities, and presentations to local small business groups.

- **Tax Identity Theft Awareness Week.** As part of Tax Identity Theft Awareness Week, the FTC held webinars to alert consumers, tax professionals, veterans, and small businesses to ways they can minimize their risk of tax identity theft, and recover if it happens. In 2019, the FTC also joined the U.S. Department of Veterans Affairs, AARP Fraud Watch Network, and the Identity Theft Resource Center to discuss tax identity theft and IRS imposter scams.

- **Mobile Device Privacy & Security.** In 2019, the FTC created new online consumer education about Mobile Payment Apps and updated guidance on how to protect your phone and the data on it. The agency also published blogs on SIM card swap scams, as well as how to protect your personal information when upgrading your phone.

- Green Lights & Red Flags: FTC Rules of the Road for Business Seminar. In August, the FTC held a Rules of the Road workshop in Atlanta, covering data security, truth in advertising, antitrust law basics, and other compliance topics. More than 200 business executives, in-house counsel, law firm practitioners, and ad agency personnel attended. The FTC hosted the day-long program in conjunction with the Office of the Georgia Attorney General, the State Bar of Georgia Antitrust Law Section, and the Better Business Bureau Serving Metro Atlanta.

- **Identity Theft Program.**
The FTC updated its military identity theft publication to reflect the new right to

free online credit monitoring for active duty military. In 2019, the FTC also participated in more than 40 identity theft-related outreach events, including: speaking at several national conferences on cybercrime and older adults; training Capital One attorneys at a Pro Bono Identity Theft Clinic; speaking at Credit Builders Alliance and World Elder Abuse Awareness Week events; and participating in numerous AARP webinars and tele-town halls. In addition, the agency worked with the Social Security Administration (SSA) to address Social Security imposters and set up IdentityTheft.gov/SSA to help people who get these scam calls. The FTC also worked with AARP to create three videos aimed at Asian American Pacific Islander older adults, helping them avoid IRS imposters, robocalls, and Medicare scams.

In 2019, the FTC participated in more than 40 identity theft-related outreach events.

- **Consumer Blog.** The FTC's Consumer Blog alerts readers to potential privacy and data security hazards and offers tips to help them protect their information. In 2019, the most-read consumer blog posts addressed how to avoid Social Security Administration imposters and how to file claims related to the Equifax settlement. In 2019, more than 50 consumer blogs addressed privacy issues, including a Parental Advisory on Dating Apps; hot topics, such as how to avoid BitCoin blackmail; and discussions of new rights, like child credit freezes and free online credit monitoring for active duty military.

- **Business Blog.** The FTC's Business Blog addresses recent enforcement actions, reports, and guidance. In 2019, there were 44 data security and privacy posts published on the Business Blog. Highlights include: guidance for YouTube channel owners on how to determine if their content is directed to children; analysis of landmark settlements like Facebook and Equifax; a series by the Director of the FTC's Bureau of Consumer Protection on small business cybersecurity; and discussion of emerging issues like genetic testing kits, voice cloning, and stalking apps.

INTERNATIONAL ENGAGEMENT

Part of the FTC's privacy and security work is engaging with international partners. The agency works with foreign privacy authorities, international organizations, and global privacy authority networks to develop mutual enforcement cooperation on privacy and data security investigations. The FTC also plays a role in advocating for 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 mechanisms developed pursuant to the U.S. SAFE WEB Act, which authorizes the FTC, in appropriate cases, to share information with foreign law enforcement authorities and to provide them with investigative assistance using the agency's statutory evidence-gathering powers. Significant enforcement cooperation developments in 2019 include:

- The FTC collaborated with the United Kingdom's Information Commissioner's Office in its actions against Cambridge Analytica and Aleksandr Kogan and Alexander Nix, described above. To facilitate international cooperation in these cases, the FTC relied on key provisions of the U.S. SAFE WEB Act, which allows the FTC to share information with foreign counterparts to combat deceptive and unfair practices.

- As part of its work on the management committee of the Global Privacy Enforcement Network (GPEN), the FTC helped to organize a series of teleconference calls and an in-person workshop on accountability and enforcement for GPEN participants. During 2019, GPEN grew to include 69 privacy authorities from 50 countries, with more than 450 staff from participating agencies registered on an internal GPEN discussion forum.

Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data transferred across national borders. It also works to promote global interoperability among privacy regimes and better accountability from businesses involved in data transfers.

During the past year, in addition to participating in the third Annual Review of the EU-U.S. Privacy Shield Framework, the FTC played an important role in policy deliberations and projects on privacy and data security internationally. For example, the FTC participated in meetings and activities of the APEC Electronic Commerce Steering Group, the International Working Group on Data Protection in Telecommunications, and the Organisation for Economic Co-operation and Development (OECD), providing input on issues ranging from children's privacy to health-related privacy to the interoperability of privacy regimes.

The FTC also engaged directly with numerous counterparts on privacy and data security issues. The Commission hosted delegations and engaged in bilateral discussions with officials from Chile, Japan, South Korea, Vietnam, and the United Kingdom; the European Commission; members of the European Parliament; and European data protection authorities.

Additionally the FTC conducted technical cooperation missions on privacy and cross-border data transfer issues in India and Brazil.

Federal Trade Commission
ftc.gov

1923172

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Rebecca Kelly Slaughter, Acting Chair
Noah Joshua Phillips
Rohit Chopra
Christine S. Wilson

In the Matter of **EVERALBUM, INC., also d/b/a EVER and PARAVISION, a corporation.**	**DOCKET NO. C-4743**

COMPLAINT

The Federal Trade Commission, having reason to believe that Everalbum, Inc., a corporation ("Respondent"), has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Everalbum, Inc. ("Everalbum"), also doing business as Ever and Paravision, is a Delaware corporation with its principal office or place of business at 1160 Gorgas Ave., San Francisco, California 94129.

2. The acts and practices of Respondent alleged in this Complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

EVERALBUM'S BUSINESS PRACTICES

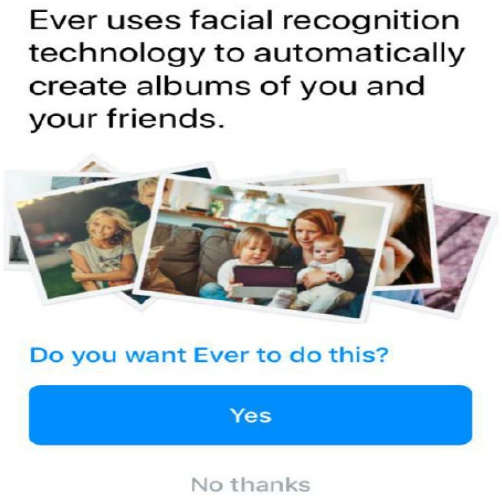
3. Since 2015, Everalbum has provided Ever, a photo storage and organization application, to consumers. Ever is available as both an iOS and Android mobile application ("app"), as well as in a web and desktop format. Globally, approximately 12 million consumers have installed Ever.

4. Ever allows consumers to upload photos and videos to Ever's cloud servers from sources such as the user's mobile device, computer, or accounts with social media services, such as Facebook or Instagram, or cloud-based storage services, such as Dropbox or One Drive. By storing photos and videos on Ever's servers, consumers can free up storage space on their devices. Ever uses automated features to organize users' photos and videos into albums by location and date.

The Ever App's Face Recognition Feature

5. In February 2017, Everalbum launched its "Friends" feature, which operates on both the iOS and Android versions of the Ever app. The Friends feature uses face recognition to group users' photos by faces of the people who appear in the photos. The user can choose to apply "tags" to identify by name (e.g., "Jane") or alias (e.g., "Mom") the individuals who appear in their photos. These tags are not available to other Ever users. When Everalbum launched the Friends feature, it enabled face recognition by default for all users of the Ever mobile app. At that time, Everalbum did not provide users of the Ever mobile app an option to turn off or disable the feature.

6. Starting in May 2018, Everalbum rolled out a process through which Ever presented Ever mobile app users located in Texas, Illinois, Washington, or the European Union with a pop-up message that, as shown below, requests that those users choose whether they would like the Ever application to use face recognition. In so doing, Everalbum disabled the Friends feature and face recognition for those users unless and until they clicked "Yes" to turn on the Friends feature and face recognition. At the same time, Everalbum also introduced into the Ever mobile app a setting that allowed users located in Texas, Illinois, Washington, or the European Union to turn on or off the face recognition feature.



7. In April 2019, Everalbum rolled out to Ever mobile app users located outside of Texas, Illinois, Washington, and the European Union the pop-up message requesting that users choose whether they would like the Ever application to use face recognition. This functioned identically to the pop-up message previously provided to users located in Texas, Illinois, Washington, and the European Union. That is, Everalbum disabled the Friends feature and face recognition unless and until the users clicked "Yes" to turn on the Friends feature and face recognition. At this time, Everalbum also rolled out to all Ever mobile app users the setting that allows users to turn on or off face recognition.

8. Since Everalbum has presented Ever mobile app users with the pop-up message requesting that users choose whether they would like the Ever application to use face recognition, approximately 25% of the approximately 300,000 users who made a selection when presented with the pop-up message chose to turn face recognition off.

9. Since July 2018, Everalbum has posted in the "Help" section of its website, everalbum.com, an article entitled *What is Face Recognition*? That article includes the following statements:

> *When face recognition is enabled*, the technology analyzes the photos and videos that you upload to create a string of numbers that we call a "face embedding" (emphasis added).
>
> ***
>
> *When face recognition is turned on, you are letting us know* that it's ok for us to use the face embeddings of the people in your photos and videos, including you, and that you have the approval of everyone featured in your photos and videos (emphasis added).

10. However, prior to April 2019, Ever mobile app users who were located anywhere other than Texas, Illinois, Washington, and the European Union did not need to, and indeed could not, take any affirmative action to "let[Everalbum] know" that it should apply face recognition to the users' photos. In fact, for those users, face recognition was enabled by default and the users lacked the ability to disable it. Thus, the article was misleading for Ever mobile app users located outside of Texas, Illinois, Washington, and the European Union.

Everalbum's Use of Ever Users' Photos to Train Its Face Recognition Technology

11. Everalbum's application of face recognition to photos uploaded by Ever mobile app users, in some cases without affirmative express consent, was not limited to providing the Friends feature. When Everalbum initially launched the Ever app's Friends feature in February 2017, the company used publicly available face recognition technology to power the feature. However, the company quickly began developing its own face recognition technology, including, in four instances, by using images it extracted from Ever users' photos to attempt to improve the technology.

12. Between September 2017 and August 2019, Everalbum combined millions of facial images that it extracted from Ever users' photos with facial images that Everalbum obtained from publicly available datasets in order to create four new datasets to be used in the development of its face recognition technology. In each instance, Everalbum used computer scripts to identify and compile from Ever users' photos images of faces that met certain criteria (i.e., not associated with a deactivated Ever account, not blurry, not too small, not a duplicate of another image, associated with a specified minimum number of images of the same tagged identity, and, in three of the four instances, not identified by Everalbum's machines as being an image of someone under the age of thirteen).

13. When compiling the second dataset in April 2018, in addition to applying the criteria described in paragraph 12, Everalbum did not include any facial images extracted from the photos of Ever users Everalbum believed to be residents of either the United States or European Union based on the users' IP addresses.

14. After testing it, Everalbum discarded the face recognition technology that it developed in the Fall of 2017 and April 2018 using the first two datasets it had compiled by combining facial images it had extracted from Ever user' photos with facial images obtained from publicly available datasets.

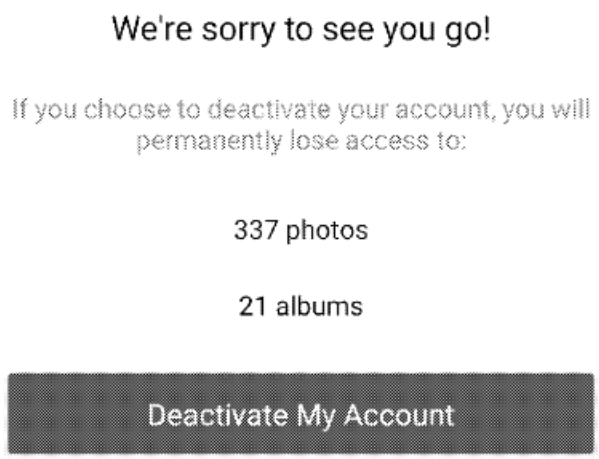
15. When compiling the third dataset in June 2018, in addition to applying the criteria described in paragraph 12, Everalbum excluded facial images extracted from the photos of Ever users Everalbum believed to be residents of Illinois, Texas, Washington, or the European Union based on the users' IP addresses. In this instance, Everalbum submitted the resulting face recognition technology to the National Institute of Science and Technology for accuracy testing and comparison to competing face recognition technologies.

16. When compiling the fourth dataset in August 2019, in addition to applying the criteria described in paragraph 12, Everalbum excluded facial images extracted from the photos of Ever users who had not either turned on the setting, or clicked "Yes" on the pop-up message, described in paragraphs 6-7 above. Everalbum used the resulting face recognition technology both in the Ever app and to build the face recognition services offered by its enterprise brand, Paravision (formerly Ever AI). Paravision offers its face recognition technology to enterprise customers for purposes such as security, access control, and facilitating payments. Everalbum has not shared images from Ever users' photos or Ever users' photos, videos, or personal information with Paravision's customers.

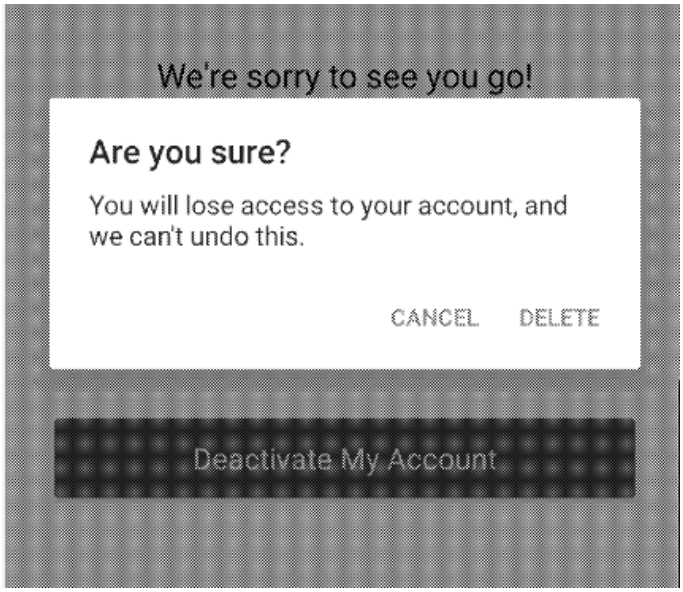
Everalbum's Account Deactivation Process

17. Everalbum offers users who no longer wish to use Ever the ability to deactivate their Ever accounts. Since January 2017, approximately 36,000 Ever users have deactivated their accounts.

18. As shown below, when a user chooses to deactivate their Ever account, Everalbum displays a message that tells the user: "We're sorry to see you go! If you choose to deactivate your account, you will permanently lose access to [##] photos and [##] albums." (The message specifies the numbers of photos and albums stored in the user's Ever account.) The message includes a button for the user to click to deactivate their account.



19. If the user clicks the "Deactivate My Account" button, as shown below, Everalbum then displays a second message stating: "Are you sure? You will lose access to your account and we can't undo this." That message includes buttons that present the user with the choice to "CANCEL" or "DELETE."



20. In response to customer inquiries about deleting an Ever account, in multiple instances, Everalbum has stated: "[Y]ou can deactivate your account at any time by signing into our app, going to 'Settings' > 'General Settings' > 'Deactivate'. *Please note that this will permanently delete all photos and videos stored on your account as well*" (emphasis added).

21. Everalbum's Privacy Policy also states:

> If you wish to deactivate your account or request that we no longer use your information to provide you any services or certain services, such as our Friends feature or our face recognition services, you can do that via your account settings, or you can email us at privacy@everalbum.com. Please understand that we may need to retain and use your information for a certain period of time to comply with our legal obligations, resolve disputes, and enforce our agreements. Consistent with these requirements, *we will try to delete your information as soon as possible upon request*. Please note, however, that there might be latency in deleting information from our servers and backed-up versions might exist after deletion (emphasis added).

22. Contrary to the statements Everalbum has made that account deactivation will result in Everalbum deleting the user's photos and videos, until at least October 2019, Everalbum did not, in fact, delete the photos or videos of any users who had deactivated their accounts and instead retained them indefinitely. Everalbum began implementing in October 2019 a practice of deleting all the photos and videos associated with Ever accounts that have been deactivated for more than three months.

Count I
Misrepresentation Regarding Ever Users' Ability to Control the Ever App's Face Recognition Feature

23. As described in Paragraph 9, Respondent represented, directly or indirectly, expressly or by implication, that Everalbum was not using face recognition unless the user enabled it or turned it on.

24. In fact, as set forth in Paragraphs 5-8 and 10, until April 2019, Everalbum was using face recognition by default for all Ever mobile app users who were located anywhere other than Texas, Illinois, Washington, and the European Union and did not provide those users with a setting to use the app and turn off face recognition. Therefore, the representation set forth in Paragraph 9 is false or misleading.

Count II
Misrepresentation Regarding Deletion of Ever Users' Photos Upon Account Deactivation

25. As described in Paragraphs 18-21, Respondent has represented, directly or indirectly, expressly or by implication, that Everalbum would delete Ever users' photos and videos upon users' deactivation of their accounts.

26. In fact, as set forth in Paragraph 22, until October 2019, Everalbum did not delete any Ever users' photos and videos upon account deactivation and instead stored them indefinitely. Therefore, the representation set forth in Paragraphs 18-21 is false or misleading.

Violations of Section 5

27. The acts and practices of Respondent as alleged in this Complaint constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this 6th day of May, 2021, has issued this Complaint against Respondent.

By the Commission.

April J. Tabor
Secretary

SEAL:

1923172

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Rebecca Kelly Slaughter, Acting Chair**
Noah Joshua Phillips
Rohit Chopra
Christine S. Wilson

In the Matter of **EVERALBUM, INC., also d/b/a EVER and PARAVISION, a corporation.**	**DECISION AND ORDER** **DOCKET NO. C-4743**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of thirty (30) days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is Everalbum, Inc., also d/b/a Ever and Paravision, a Delaware corporation with its principal office or place of business at 1160 Gorgas Ave., San Francisco, California 94129.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "Affected Work Product" means any models or algorithms developed in whole or in part using Biometric Information Respondent collected from Users of the "Ever" mobile application.

B. "Biometric Information" means data that depicts or describes the physical or biological traits of an identified or identifiable person, including depictions (including images), descriptions, recordings, or copies of an individual's facial or other physical features (e.g., iris/retina scans), finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern).

C. "Clearly and Conspicuously" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

D. "Covered Information" means information from or about an individual consumer, including: (1) a first and last name; (2) a physical address; (3) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial account number; (8) credit or debit card information; (9) photos and videos; (10) Biometric Information; (11) descriptive information derived from Biometric Information, including a Face Embedding; (12) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, processor serial number, user ID, or any other persistent identifier that can be used to recognize a user over time and/or across different devices, websites or online services; or (13) any information combined with any of (1) through (12) above.

E. "Face Embedding" means data, such as a numeric vector, derived in whole or in part from an image of an individual's face.

F. "Respondent" means Everalbum, Inc., also doing business as Ever and Paravision, and its successors and assigns.

G. "User" means a person who has downloaded, accessed, and/or used software, such as a mobile application, developed, operated, or offered by Respondent and marketed to consumers for personal use, including the "Ever" mobile application.

Provisions

I. Prohibition against Misrepresentations

IT IS ORDERED that Respondent; and Respondent's officers, agents, and employees; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service must not misrepresent in any manner, expressly or by implication:

A. The extent to which Respondent collects, uses, discloses, maintains, or deletes any Covered Information;

B. The extent to which consumers can control the collection, use, disclosure, maintenance, or deletion of Covered Information;

C. The extent to which Respondent accesses or permits access to Covered Information;

D. The extent to which, purposes for which, or duration of time during which Respondent retains any Covered Information following a consumer's deletion or deactivation of a user account with Respondent; or

E. The extent to which Respondent otherwise protects the privacy, security, availability, confidentiality, or integrity of any Covered Information.

II. Notice and Affirmative Express Consent Provision

IT IS FURTHER ORDERED that Respondent; and Respondent's officers, agents, and employees; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, prior to using Biometric Information collected from a User to (1) create a Face Embedding or (2) train, develop, or alter any face recognition model or algorithm, must:

A. Clearly and Conspicuously disclose to the User from whom Respondent has collected the Biometric Information, separate and apart from any "privacy policy," "terms of use" page, or other similar document, all purposes for which Respondent will use, and to the extent applicable, share, the Biometric Information; and

B. Obtain the affirmative express consent of the User from whom Respondent collected the Biometric Information.

Provided, however, Respondent need not comply with this provision in connection with any product or service that is only offered to Users outside the United States.

III. Deletion

IT IS FURTHER ORDERED that Respondent; and Respondent's officers, agents, and employees; and all other persons in active concert or participation with any of them, who receive actual notice of this Order, must, unless prohibited by law:

A. Within thirty (30) days after the issuance date of this Order, delete or destroy all photos and videos that Respondent collected from Users who requested deactivation of their Ever accounts on or before the issuance date of this Order, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed;

B. Within ninety (90) days after the issuance of this Order, delete or destroy all Face Embeddings derived from Biometric Information Respondent collected from Users who have not, by that date, provided express affirmative consent for the creation of the Face Embeddings, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed; and

C. Within ninety (90) days after the issuance of this Order, delete or destroy any Affected Work Product, and provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction.

Provided, however, that any photos, videos, Face Embeddings, Affected Work Product, or other matter that Respondent is otherwise required to delete or destroy pursuant to this provision may be retained, and may be disclosed, as requested by a government agency or otherwise required by law, regulation, court order, or other legal obligation, including as required by rules applicable to the safeguarding of evidence in pending litigation. In each written statement to the Commission required by this provision, Respondent shall describe in detail any relevant information that Respondent retains on any of these bases and the specific government agency, law, regulation, court order, or other legal obligation that prohibits Respondent from deleting or destroying such information. Within thirty (30) days after the obligation to retain the information has ended, Respondent shall provide an additional written statement to the Commission, sworn under penalty of perjury, confirming that Respondent has deleted or destroyed such information.

IV. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within ten (10) days after the issuance date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten (10) years after the issuance date of this Order Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives having managerial responsibilities for conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

V. Compliance Reports and Notices

IT IS FURTHER ORDERED that Respondent make timely submissions to the

Commission:

A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (b) identify all of the Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, what Covered Information is collected, and the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (a) any designated point of contact or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (14) days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Everalbum, Inc., FTC File No. 1923172."

VI. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for ten (10) years after the issuance date of the Order, and retain each such record for five (5) years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;

D. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security, availability, confidentiality, or integrity of any Covered Information, including any representation concerning a change in any website, mobile app, or other service controlled by Respondent that relates to privacy, security, availability, confidentiality, or integrity of Covered Information; and

E. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

VII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

VIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its

publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than twenty (20) years;

B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:

ISSUED: May 6, 2021

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 92975 / September 14, 2021

ADMINISTRATIVE PROCEEDING
File No. 3-20549

In the Matter of **App Annie Inc. and Bertrand Schmitt,** **Respondents.**	**ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission ("Commission" or "SEC") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 21C of the Securities Exchange Act of 1934 ("Exchange Act") against App Annie Inc. and Bertrand Schmitt ("Respondents").

II.

In anticipation of the institution of these proceedings, Respondents have submitted Offers of Settlement (the "Offers") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over them and the subject matter of these proceedings, which are admitted, and except as provided herein in Section V, Respondents consent to the entry of this ("Order"), as set forth below.

III.

On the basis of this Order and Respondents' Offers, the Commission finds that:

SUMMARY

1. App Annie Inc. ("App Annie" or the "Company") is one of the largest sellers of market data on how apps on mobile devices are performing, including data on the number of times

a particular company's app is downloaded, the amount of revenue that a company is generating through its app, and how often customers are using that company's app. Trading firms commonly refer to this type of information as "alternative data," i.e., information about companies or investments that is not contained within financial statements or other traditional data sources. Many trading firms pay for subscriptions to alternative data sources like App Annie and use this alternative data in making investment decisions. Between late 2014 and mid-2018 (the "relevant period"), App Annie and its co-founder and former CEO and Chairman Bertrand Schmitt ("Schmitt") violated the antifraud provisions of the federal securities laws by making material misrepresentations about how App Annie's alternative data was derived, and engaging in other deceptive practices, in order to induce trading firms to become and remain subscribers for the purpose of using App Annie's data in their decisions to purchase and sell securities.

2. App Annie provides a free analytics product called "Connect" to companies that offer apps, including public companies, which enables those companies to track how their apps are performing. As a condition of their use of Connect, those companies provide App Annie with their app store credentials to allow App Annie to collect their confidential app performance metrics ("Connect Data"). App Annie tells Connect users that it will generate estimates of app performance using their Connect Data, but that it will only use Connect Data in aggregated and anonymized form to generate those estimates.

3. App Annie sells estimates of app performance through a separate subscription product called "Intelligence." During the relevant period, more than 100 trading firms paid for Intelligence subscriptions to obtain estimates for use in making investment decisions. App Annie and Schmitt represented to Intelligence subscribers that Intelligence estimates were generated through a statistical model that used aggregated and anonymized Connect Data, and that Connect users had consented to App Annie using their confidential data in this way. Contrary to these representations, however, during the relevant period App Annie used confidential Connect Data, in its non-aggregated and non-anonymized form, to alter Intelligence estimates generated by the statistical model in order to make the estimates closer to Connect users' actual app metrics, and thereby more valuable to App Annie to sell.

4. App Annie and Schmitt also represented to subscribers that the Company had internal controls and processes to prevent the misuse of confidential Connect Data and to ensure that App Annie was in compliance with the federal securities laws. For example, they represented that public companies' Connect Data was not used to generate Intelligence estimates. They understood that, without these representations, trading firm subscribers would not have purchased or used App Annie's Intelligence estimates in making their trading decisions. During most of the relevant period, however, App Annie did not have effective internal controls and in fact used certain public companies' Connect Data to generate Intelligence estimates.

5. Through their misrepresentations and other deceptive practices, App Annie, led by Schmitt, misled Intelligence subscribers about how the Company's Intelligence estimates were generated during the relevant period. As a result of their misconduct, App Annie and Schmitt violated Section 10(b) of the Exchange Act and Rule 10b-5 thereunder.

RESPONDENTS

6. **App Annie Inc.** is a private Delaware corporation with its principal place of business in San Francisco, California. The Company was co-founded in 2010 by Bertrand Schmitt. During the relevant period, App Annie had between 250 and 400 employees, located in multiple offices around the world. Since its founding, App Annie has sold estimates of companies' app revenue, app downloads, and app usage to companies that offer apps and to trading firms, and has become a leading alternative data provider with respect to mobile app performance data. App Annie has advertised that it provides the most accurate app performance estimates in the industry because it is able to access confidential app performance metrics from over a million apps that are connected to its free app analytics product, Connect.

7. **Bertrand Schmitt** is a co-founder of App Annie and was its CEO from 2010 until June 2018, when he resigned and the Board replaced him as CEO. Schmitt served as Chief Strategy Officer of App Annie from June 2018 until January 2020, when his employment was terminated. Schmitt also was formerly a member of the Board of Directors and served as Chairman of the Board from the Company's founding until January 2021, when he stepped down as Chairman. Schmitt, 45 years old, is a resident of Mercer Island, Washington.

FACTS

A. Background

8. Many companies – including publicly traded companies in the entertainment, gaming, social media, travel, fitness, food, and retail sectors – make apps available for their customers to download and use on their mobile devices, including smartphones and tablets. Many of these companies also sell products, services, or advertisements through their apps. Details concerning how often a company's app is downloaded, how much revenue is generated by app purchases and in-app purchases, and how often its app is used is confidential, nonpublic data belonging to the company, and often is material to a public company's financial performance and stock price.

9. Since its founding, App Annie has offered a free app analytics product called "Connect" (formerly called "Analytics") to companies that offer apps. Connect enables these companies to visualize and track how their apps are performing. In order to use the Connect product, companies provided App Annie with their app store login credentials so that App Annie could collect their confidential app performance data.

10. During the relevant period, App Annie did not enter into individual contracts with Connect users; rather, it was bound by the Terms of Service posted on its website, which described how App Annie could use the confidential app performance data collected with the Connect users' app store credentials.

11. Schmitt understood that companies would not sign up to use the Connect product unless App Annie promised that their confidential app performance data would not be disclosed to

third parties. As a result, Schmitt and others at App Annie designed the Terms of Service to assure Connect users that there would be limitations on the ways that App Annie could use their data. Specifically, the Terms of Service stated that App Annie could use Connect Data to generate "estimates" of how apps in certain categories were performing, but that the estimates would be generated by App Annie's statistical model "from aggregated pools of information" in order to make their data "non-identifiable."

12. In communications with Connect users, App Annie employees made similar representations about the limited way in which data collected from Connect users could be used by the Company. For example, App Annie representatives were trained to respond to inquiries from Connect users about how their data would be used by representing that Connect Data would be "aggregated" and "anonymized" before being entered into a "statistical model" that generated "estimates."

13. App Annie's business model relied on selling estimates of how apps belonging to certain companies were performing. App Annie sold these estimates through a paid subscription product called "Intelligence," which included "Store Intelligence" (for estimates of app revenue and app downloads) and "Usage Intelligence" (for estimates of app usage). Paying subscribers were companies that offered apps and trading firms, such as hedge funds. During the relevant period, substantially all of App Annie's revenue was derived from selling Intelligence estimates to these subscribers.

B. App Annie and Schmitt Encouraged Trading Firms to Use Its Estimates in Making Investment Decisions

14. As part of their investment decision-making process, many trading firms subscribe to alternative data sources. Alternative data can include data compiled from mobile devices, financial transactions, satellites, public records, and the internet, among other sources. During the relevant period, App Annie became the leading alternative data provider with respect to mobile app performance data. App Annie advertised that, just as Nielsen provided market data for television ratings and Comscore provided market data for websites, App Annie was the leader in providing market data for mobile apps.

15. During the relevant period, more than 100 trading firms paid for App Annie's Intelligence subscription products in order to obtain estimates of how apps belonging to certain companies were performing, and App Annie encouraged trading firms to make investment decisions based on Intelligence estimates. For example, App Annie's marketing materials encouraged "investors" and "finance professionals" to use Intelligence estimates to "inform their investment strategy." App Annie's website claimed that investors could "make more informed decisions about existing positions" by "benchmark[ing] the performance of public app companies against key metrics including user engagement, revenue and growth." Schmitt occasionally participated in meetings with existing and prospective trading firm subscribers, and some of the materials used in these meetings pitched that Intelligence estimates could help with "financial modeling," "sharpen earnings forecasts with estimated downloads and revenue inputs," and "identify investment opportunities." Schmitt approved many of these marketing materials.

16. App Annie's sales representatives and customer success representatives (whose role was to retain and up-sell existing customers) encouraged prospective and existing trading firm subscribers to make investment decisions based on Intelligence estimates and presented "investor case studies" that touted how closely App Annie's estimates correlated with certain public companies' publicly reported metrics and stock prices. App Annie hired customer success representatives with trading firm experience to build relationships with these subscribers and to demonstrate how to generate value from their Intelligence subscriptions. For example, these representatives generated and shared "use case" ideas for how trading firms could use Intelligence estimates to trade ahead of upcoming earnings announcements.

17. During the relevant period, trading firms told Schmitt and others at App Annie that they were making investment decisions based on Intelligence estimates, and trading firms were in fact buying and selling securities based on estimates they purchased from App Annie. Based on his understanding of the value that trading firms were deriving from Intelligence estimates, Schmitt had App Annie charge trading firms a higher subscription price than other Intelligence subscribers.

C. App Annie and Schmitt Assured Trading Firms and Connect Users that App Annie's Use of Confidential Data Complied with the Federal Securities Laws

18. Throughout the relevant period, Schmitt understood it was material to trading firms' decisions to use App Annie's estimates for investment purposes both that the Intelligence estimates they were purchasing did not constitute material nonpublic information under the federal securities laws and that App Annie was using Connect Data in a way that was consistent with Connect users' consent.

19. Schmitt reassured App Annie's customer-facing employees (such as those in the Sales, Marketing, and Customer Success departments) and many of App Annie's trading firm subscribers that the Company abided by its Terms of Service by affirming that Intelligence estimates were derived through a statistical model that utilized "aggregated" and "anonymized" Connect Data combined with certain publicly available information.

20. Schmitt and others at App Annie provided additional reassurance to trading firm subscribers by representing that the Company had processes and internal controls in place to ensure that it was not selling them material nonpublic information in violation of the federal securities laws. For example, they represented that the Company was conducting regular reviews to ensure compliance with legal requirements governing the handling and use of material nonpublic information. Schmitt made similar representations at meetings with trading firms and at trading firm conferences.

21. App Annie and Schmitt made these representations as part of an effort to sell Intelligence subscriptions to trading firms, in response to diligence questionnaires from trading firms, or to persuade trading firm subscribers not to switch to App Annie's competitors.

22. Yet during the relevant period, the Company did not have effective internal controls and did not conduct regular compliance reviews, and representations to the contrary were false and misleading.

D. App Annie Failed to Exclude Confidential Public Company Data from its Estimate Generation Process

23. In or around late 2014, Schmitt and App Annie began representing to trading firms that were prospective or existing Intelligence subscribers that the Company had internal controls in place to prevent App Annie from selling material nonpublic information it obtained from public companies to Intelligence subscribers. For example, App Annie represented that public company Connect Data was not used by the Company's statistical model to generate Intelligence estimates.

24. While Schmitt agreed, around this time, to an internal policy whereby certain public company Connect Data would be excluded from the Company's statistical model, he failed to direct anyone at App Annie to document any such policy until April 2017. When App Annie first documented a policy restricting the use of public company Connect Data in April 2017, the policy only required that the statistical model exclude app *revenue* data from *certain* public companies (*i.e.*, those whose app revenue exceeded 5% of the company's total revenue), and placed no limitations on the input of app *download* and app *usage* data from public companies into the statistical model.

25. Even after the policy was documented in April 2017, Schmitt and App Annie failed to take steps to ensure that the policy was properly implemented. It was only in June 2018, after the Company learned of the SEC's investigation, that App Annie amended the policy to fully exclude public company Connect Data from its estimate generation process and took steps to implement the amended policy.

26. During the relevant period, Schmitt repeatedly assured other App Annie executives that the Company's use of confidential Connect Data complied with the federal securities laws because a policy prohibiting the use of certain public company Connect Data in preparing estimates was in place and was being followed. Schmitt and others at App Annie gave similar assurances to trading firm subscribers in response to inquiries about what internal controls App Annie had in place to prevent the sale of material nonpublic information. They also gave similar assurances to Connect users that were public companies in response to inquiries about how their data would be used by App Annie. However, these representations about App Annie's internal controls were not accurate and all app download data, all app usage data, and certain app revenue data from public companies were used in App Annie's statistical model to generate Intelligence estimates during the relevant period.

E. Schmitt Approved App Annie Employees' Use of Non-Anonymized and Non-Aggregated Confidential Data to Alter Estimates

27. As App Annie's co-founder and CEO, Schmitt was closely involved in building the products that the Company offered during the relevant period, including its free Connect product and its paid Intelligence products.

28. Schmitt was viewed as a "Product CEO" by employees, and Schmitt remained closely involved in major decisions about the Store Intelligence product in particular, even as the Company grew in size and began offering additional paid products. During the relevant period, Schmitt was considered the Company's expert on the statistical model underlying the Store Intelligence product because he had helped develop it.

29. Given its importance to the success of the Company, Schmitt was acutely focused on how close App Annie's Intelligence estimates were to actual app performance figures, as this was the primary way that App Annie could distinguish itself from competitors and increase its subscription revenues. App Annie carefully tracked how close the Company's Intelligence estimates were to actual app performance figures by comparing the estimates to actual confidential Connect Data. App Annie regularly touted to prospective Intelligence subscribers that its estimates of top-ranked apps' performance were the most accurate in the industry, with 80% to 90% of its estimates within 20% of actual figures.

30. Schmitt instructed App Annie employees to attract as many companies offering apps as possible to its Connect service so that App Annie could collect more actual app performance data and thereby improve the accuracy of its Intelligence estimates. Behind the scenes, however, Schmitt also directed a small number of employees to use actual app performance data in ways that were prohibited by the Connect Terms of Service to force the model-generated Intelligence estimates closer to the actual figures before they were delivered to subscribers.

Schmitt Approved App Annie's Creation and Use of a Manual Estimate Alteration Process

31. Beginning at least in 2014, in an effort to make the Intelligence estimates closer to the actual app performance metrics, App Annie created a manual process whereby a "Delivery Team," which consisted of a subset of App Annie engineers based in Beijing, China, made manual alterations to estimates generated by the statistical model before they were delivered to Intelligence subscribers. Schmitt was aware of and approved the creation and use of this manual alteration process.

32. The Delivery Team manually altered the estimates for apps that were of greatest interest to App Annie's highest-paying subscribers. When App Annie received complaints from subscribers about the inaccuracy of a particular company's app performance estimates, the Delivery Team was tasked with improving the estimates through this manual process.

33. To make these manual alterations, the Delivery Team looked at confidential Connect Data, including public company app performance data. The Delivery Team was not trained or supervised by anyone in the Company's Data Science group and did not document which estimates were adjusted or what changes were made. There was no statistical basis for these post-model alterations. The only purpose of these alterations was to make the estimates closer to the actual metrics.

34. Schmitt approved the creation and use of this manual alteration process because he believed it was cheaper and more effective at making the estimates closer to the actual results than a process that would have complied with the Connect Terms of Service, such as having data scientists research and implement improvements to the statistical model itself.

35. These manual alterations continued throughout the relevant period. Whenever Schmitt had concerns about the Intelligence estimates deviating too far from the actual app performance figures, he expanded these practices and more Delivery Team engineers were hired to engage in manual alterations for a greater number of apps.

36. Schmitt and the Delivery Team never shared with other App Annie executives, Intelligence subscribers, Connect users, or customer-facing employees (such as those in Sales, Marketing, or Customer Success) what this manual alteration process actually entailed. Some employees were told there was a "QA" (Quality Assurance) process relating to the delivery of estimates, but they were not told this involved manually altering estimates based on actual non-aggregated and non-anonymized Connect Data.

Schmitt Approved App Annie's Creation and Use of an Automated Estimate Alteration Process for Apps Belonging to Connect Users

37. Beginning in or around mid-2015 and throughout 2016, despite the manual alterations described above, Schmitt and others at App Annie became increasingly concerned that the Store Intelligence estimates were deviating too far from the actual app performance figures of Connect users. Increasing numbers of App Annie subscribers complained about the estimates' lack of accuracy and moved to App Annie's competitors, putting the Company's revenue at risk.

38. Schmitt brought this issue up frequently at internal meetings and directed the Company's Chief Data Scientist to investigate ways to improve the statistical model underlying the Store Intelligence product so that it would produce estimates that were closer to the actual app performance figures of Connect users.

39. In or around mid-2016, the Chief Data Scientist proposed an overhaul of the Store Intelligence statistical model to improve the accuracy of the estimates it generated. Schmitt rejected the proposal because he believed it would be too expensive and time-consuming to implement, and would result in only modest improvements to the estimates. Instead, Schmitt worked with an employee responsible for the Intelligence product to explore other options for making the estimates closer to the actual Connect Data, and in or around October 2016, approved the addition of a new step in the Store Intelligence estimate delivery process called "error-halving."

40. Error-halving compared the model-generated estimates for apps belonging to Connect users with the actual performance figures for those apps (e.g., confidential revenue and download numbers that App Annie had collected for those apps using the Connect users' app store credentials), and then automatically adjusted the model-generated estimates for those apps to be closer to their actual numbers. Specifically, if the difference between the estimate generated by the model and the actual performance figure for the app was larger than a certain threshold percentage approved by Schmitt, App Annie cut the difference by half and replaced the model-generated estimate with the more accurate number.

41. Schmitt understood that error-halving made the final Intelligence estimates systematically closer to the actual numbers through post-model alterations that directly relied on Connect Data (including public company data) in a non-aggregated and non-anonymized form, rather than through a statistical estimation process.

42. Schmitt sought the Chief Data Scientist's assistance in implementing error-halving, but the Chief Data Scientist refused because it was not grounded in data science. The Chief Data Scientist informed Schmitt that he did not believe post-model alterations to app estimates were appropriate because improvements to the accuracy of the model-generated estimates should only be made through adjustments to the statistical model itself in order to improve its predictive power.

43. With Schmitt's approval but without the involvement of anyone from the Data Science team, Delivery Team engineers in Beijing implemented error-halving gradually over several months, between March 2017 and June 2017, to avoid detection by App Annie's Intelligence subscribers.

44. Schmitt and the Delivery Team did not share this estimate alteration process with other App Annie executives, Intelligence subscribers, Connect users, or customer-facing employees (such as those in Sales, Marketing, or Customer Success).

F. Schmitt Failed to Disclose the Deceptive Practices While He and Others at App Annie Continued to Disseminate Misrepresentations About the Estimate Generation Process

45. Even as App Annie employees were engaging in estimate alteration practices using non-aggregated and non-anonymized Connect Data, Schmitt and others at App Annie continued to falsely represent to trading firm subscribers and to Connect users that Intelligence estimates were generated by a statistical model that used Connect Data in "aggregated" and "anonymized" form. Schmitt knew and approved of employees describing App Annie's estimate generation process in this way, and was aware that employees were repeating these misleading claims in their communications with Intelligence subscribers and Connect users.

46. Schmitt knew, or was reckless in not knowing, that trading firm subscribers were purchasing Intelligence estimates based on App Annie's material misrepresentations and other deceptive practices concerning the estimates, and were doing so for the purpose of buying and

selling securities. These trading firm subscribers did in fact buy and sell securities based on App Annie's Intelligence estimates.

47. The above representations by Schmitt and by other App Annie employees were false and misleading because App Annie engaged in the deceptive estimate alteration practices described above, which were approved by Schmitt. These deceptive practices resulted in App Annie selling Intelligence estimates refined using confidential Connect Data to unknowing trading firm subscribers to use in their purchase and sale of securities. Moreover, because this allowed the Company to deliver estimates that were closer to the actual confidential Connect Data, and thus more attractive to subscribers, App Annie was able to retain and grow its customer base and revenue streams.

G. App Annie's Board Replaced Schmitt as CEO and App Annie Changed Its Estimate Generation Process

48. In June 2018, after the Company had learned of the SEC's investigation, App Annie discontinued all post-model estimate alteration practices based on non-aggregated and non-anonymized Connect Data. The Company also began excluding all public company data from its statistical model, consistent with its representations to Intelligence subscribers and Connect users. Around the same time, Schmitt resigned and the Board replaced him as CEO.

49. App Annie eventually implemented a new version of the statistical model underlying the Store Intelligence product that had been proposed by the Chief Data Scientist in or around mid-2016.

50. After he was replaced as CEO, Schmitt served as Chief Strategy Officer until App Annie terminated his employment in January 2020.

VIOLATIONS

51. As a result of the conduct described above, App Annie and Schmitt violated Section 10(b) of the Exchange Act and Rule 10b-5 thereunder, which prohibit fraudulent conduct in connection with the purchase or sale of securities.

IV.

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondents' Offers.

Accordingly, pursuant to Section 21C of the Exchange Act, it is hereby ORDERED that:

A. App Annie and Schmitt cease and desist from committing or causing any violations and any future violations of Section 10(b) of the Exchange Act and Rule 10b-5 thereunder.

B. Schmitt be, and hereby is, prohibited from serving or acting as an officer or director of any issuer that has a class of securities registered pursuant to Section 12 of the Exchange Act [15 U.S.C. § 78l] or that is required to file reports pursuant to Section 15(d) of the Exchange Act [15 U.S.C. § 78o(d)] for a period of three (3) years from the entry of this Order.

C. App Annie and Schmitt shall each pay a civil money penalty as follows:

(1) App Annie shall, within ten (10) days of the entry of this Order, pay a civil money penalty in the amount of $10,000,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

(2) Schmitt shall, within ten (10) days of the entry of this Order, pay a civil money penalty in the amount of $300,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

(3) Payment must be made in one of the following ways:

(a) Respondents may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(b) Respondents may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(c) Respondents may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying the Respondent, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Monique C. Winkler, Division of Enforcement, Securities and Exchange Commission, 44 Montgomery Street, Suite 2800, San Francisco, CA 94104.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondents agree that in any Related Investor Action, they shall not argue that they are entitled to, nor shall they benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondents' payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondents agree that they shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondents by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

V.

It is further Ordered that, solely for purposes of exceptions to discharge set forth in Section 523 of the Bankruptcy Code, 11 U.S.C. § 523, the findings in this Order are true and admitted by Respondent Schmitt, and further, any debt for disgorgement, prejudgment interest, civil penalty, or other amounts due by him under this Order or any other judgment, order, consent order, decree, or settlement agreement entered in connection with this proceeding, is a debt for the violation by him of the federal securities laws or any regulation or order issued under such laws, as set forth in Section 523(a)(19) of the Bankruptcy Code, 11 U.S.C. § 523(a)(19).

By the Commission.

Vanessa A. Countryman
Secretary

LATHAM & WATKINS LLP

Global Privacy & Security Compliance Law Blog

Commentary on Global Privacy and Security Issues of Today

FTC Chair Rebecca Slaughter Outlines Data Privacy Enforcement Agenda

By Latham & Watkins LLP on February 12, 2021

Posted in Legislative & Regulatory Developments, Privacy

Slaughter discusses the FTC's priorities under the new administration, including ed-tech, health apps, and racial equity.

By Jennifer Archie, Michael Rubin, Marissa Boynton, and Jimmy Smith

On February 10, 2021, in her first major speech as acting chair of the Federal Trade Commission (the Commission, or the FTC), Rebecca Slaughter discussed the Commission's enforcement priorities under the new administration — with a particular focus on deterring problematic data practices.

In her opening remarks at the Future of Privacy Forum, Slaughter stated that she would urge innovation and creativity and the use of all tools available to the Commission in order to bring about the best outcomes for consumers and to deter problematic privacy and data security practices.[i] She also noted that enhanced enforcement around ed-tech, health apps, and racial equity would be priorities for the new administration. In particular, Slaughter mentioned two types of relief that she believes the Commission should focus on going forward: disgorgement and effective consumer notice.

Types of Relief

Disgorgement

The first type of relief that Slaughter referenced is the principle of disgorgement. Slaughter stated that the Commission has often employed the concept of disgorgement of "ill-gotten monetary gains" when consumers pay

companies for products or services that involved deceptive marketing. She used *Everalbum* as an example of how the Commission could employ disgorgement in privacy cases in which companies process data from consumers in deceptive ways.[ii] Slaughter stated that the Commission should require violators "to disgorge not only the ill-gotten data, but also the benefits" derived from such data. In the Everalbum case, Slaughter noted that such benefits included the algorithms that were generated from the data.

Effective Consumer Notice

The second type of relief that Slaughter referenced is effective consumer notice. Slaughter proposed requiring companies to notify consumers if they used consumer information inappropriately or in a way materially different from what was promised, with the hope that "consumers will 'vote with their feet'" and that such notice will allow them "to better decide whether to recommend the services to others." Slaughter added that, most critically, effective consumer notice "accords consumers the dignity of knowing what happened," and added that she will be pushing her staff to include provisions requiring consumer notice in privacy and data security orders.

As an example, Slaughter discussed the Commission's recent fem-tech case involving the Flo menstruation and fertility app, in which the Commission alleged that Flo shared consumer information with other companies, including Facebook and Google — thereby violating the promises it made to consumers that it would not share their personal information.[iii] The Commission required Flo to notify each of the affected consumers of its false promises.

Use All Tools Available

Besides disgorgement and effective consumer notice, Slaughter also stated that she wanted to ensure that all future cases brought by the Commission would include an analysis of applicable laws in order to ensure that the Commission pleads all possible violations of law. As an example, in a concurring statement (and perhaps a harbinger of what the future holds), Slaughter stated that the Commission should have included unfairness counts.[iv] Future enforcement cases could likely contain all potential pleadings cutting across a panoply of laws under the Commission's jurisdiction.

Pandemic Considerations Are Priority Number 1: Ed-Tech, Health Apps, Broadband

Slaughter further stated that she and her staff would particularly focus on ed-tech and health apps as they relate to the pandemic.

Ed-Tech

With respect to ed-tech, Slaughter stated that the Commission was conducting an industry-wide study of social media and video streaming platforms. She also noted that the Commission is in the process of reviewing the Children's Online Privacy Protection Act (COPPA) rule to clarify how COPPA applies in the ed-tech space.

Health Apps

With respect to health apps, Slaughter mentioned that she would like to see more enforcement around companies similar to Flo.

Broadband Privacy Issues

Slaughter further reported that the Commission would issue a report on an industry-wide study of broadband privacy practices.

Racial Equity Is Priority No. 2: Digital Services, Algorithms, Facial Recognition Technologies, and Geolocation Data

Slaughter stated that the Commission would make racial equity a priority issue.

Expensive Digital Services

Slaughter noted that "digital services can target vulnerable communities with unwanted content and that vulnerable communities suffer outsized consequences from data privacy violations." She stated that the Commission would examine the ways in which vulnerable communities are asked to pay with their data for expensive services that they can ill afford.

Algorithms

Slaughter further mentioned that it is essential that algorithms are not used in discriminatory ways. She stated that her staff would "actively investigate biased and discriminatory algorithms" and that she was interested in the further exploration of the best methods to redress artificial intelligence-generated consumer harms.

Facial Recognition Technologies

Slaughter stated that the Commission will redouble efforts to identify violations in the law concerning the deployment and development of facial recognition technologies.

Geolocation Data

Slaughter relayed concern about the misuse of mobile apps' use of location data generally, and especially "as it applies to tracking Americans engaged in constitutionally protected speech."

End notes

[i] Rebecca Kelly Slaughter, Acting Chairwoman, FTC, Remarks at the Future of Privacy Forum: Protecting Consumer Privacy in a Time of Crisis (Feb. 10, 2021).

[ii] Complaint ¶¶ 9, 23, 24, *In the Matter of Everalbum, Inc.*, No. 1923172 (FTC Jan. 11, 2021).

[iii] Comm'r Rohit Chopra & Comm'r Rebecca Kelly Slaughter, FTC, Joint Statement Concurring in Part, Dissenting in Part, *In the Matter of Flo Health, Inc.*, No. 1923133 (Jan. 13, 2021).

[iv] Rebecca Kelly Slaughter, Comm'r, FTC, Concurring Statement, *FTC and State of New York v. Vyera Pharmaceuticals, LLC, Phoenixus AG; Martin Shkreli; and Kevin Mulleady*, No. 161-0001 (FTC Jan. 27, 2020).

Understanding HIPAA's security rule for telemedicine apps

Dec 1, 2020 Save This ()


Heidi Wachs, CIPP/US
IAPP Member Contributor (/about/person/0011a00000DlGHhAAN)


Jeffrey Atteberry
IAPP Member Contributor (/about/person/0011a00000DlOyjAAF)


Noah Rubin
Nonmember Contributor (/about/person/0011P000017jLpzQAE)

The rapid growth in telehealth has predictably spawned the development of a variety of new software solutions to serve the needs of both doctors and patients. While the field is wide open for application developers, the area of telemedicine also presents some unique data privacy and security challenges. Of course, the principles of privacy by design tell us that data privacy concerns should be integrated into the entire design process, but this imperative becomes all the more important and challenging when the app in development will be handling users' personal information.

The U.S. Health Insurance Portability and Accountability Act imposes unique data security standards on telehealth app developers. In March, the Department of Health and Human Services temporarily suspended (https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html) enforcement for noncompliance with HIPAA rules in connection with the good-faith use of telehealth services during the pandemic.

This temporary suspension should not lead telehealth app developers into a false sense of complacency regarding HIPAA's strict security requirements. Any telehealth-specific app must comply with the HIPAA Security Rule if it is to have any meaningful market success.

Further, reduced risk of enforcement should not lead to lax security practices. The threat of bad actors exploiting weak or immature security controls to access or exfiltrate personal information, intellectual property, such as source code, or other sensitive information is ever-present. Telehealth app developers should implement best practices for security when designing and improving their apps, especially as the apps continue to iterate and new features are added.

As an initial matter, any telemedicine or telehealth app facilitating the transfer of protected health information between health care providers and patients will need to enter into a business associate agreement with the health care provider. HIPAA requires health care providers to enter into a BAA with any vendor that transmits or maintains electronically protected health information on its behalf to ensure the vendor is properly safeguarding the ePHI. Through the BAA, the vendor represents that its services will comply with HIPAA's Privacy, Security, Breach Notification and Enforcement Rules as applicable to the services being provided.

HIPAA's Security Rule

HIPAA's Security Rule sets standards for administrative, physical, technical and organizational safeguards to secure protected health information. The technical safeguards specifically identify policies and procedures for protecting ePHI and controlling access to it and fall into the following categories: access control, audit controls, data integrity, authentication and transmission security.

Access control

HIPAA requires the implementation of policies and procedures to ensure that only authorized persons and software programs access the ePHI. The Security Rule does not specify any particular technical controls for meeting this standard; however, it does set forth two required implementation specifications that an app developer must meet and two more that should be implemented when reasonable and appropriate. In the context of app development, all four specifications should be implemented.

Unique user ID

Each user of the app should be assigned a globally unique identifier, which can be a username, number or random string of characters. Using this GUID, the system should be able to attribute and protect access to app-related data for end users (patients and health care providers), as well as employees or vendors. GUIDs as a method of identification, however, should not be conflated with authentication, which is detailed further below. Systems should require more than just a GUID to provide access, as they may be publicly available or easily ascertained.

Emergency access procedures

Generally speaking, the Security Rule requires that the system establish and implement as needed a procedure for obtaining necessary ePHI in an emergency situation.

Automatic logoff

The app must also implement electronic procedures that terminate authenticated sessions after a predetermined time of inactivity. An automatic logoff system reduces the risk that unauthorized users will gain access to the system and related ePHI. Although it can create a bit of a speed bump in the user experience, telehealth app developers should seek to shorten the inactivity period that triggers the automatic logoff, particularly for web apps.

Encryption and decryption

Where feasible, encryption should be used to protect ePHI from unauthorized access either by individuals or other software programs. Using standard protocols like HTTP with TLS protects data in transit, and modern encryption schemes, like advanced encryption standard and authenticated encryption, protect data at rest.

Technical means must be implemented for recording and examining activity on the system. Audit controls also typically include the ability to generate an audit report. Such capabilities are particularly important for gathering system information in the event of a security violation. The Security Rule does not specify what data must be gathered by the audit controls. Consequently, app developers should consider what data is collected, how the system is used and what kind of security breaches are more likely when designing the audit controls. Importantly, app developers should also be mindful of the ways in which audit controls can, if not well designed, introduce additional security risks.

In addition to audit controls, app developers should ensure they have implemented monitoring and alerting on the app's underlying infrastructure to identify any anomalous behavior. The first step to understanding events that occur on application infrastructure is to collect them in a centralized location. Having a security incident and event management system allows companies to collect disparate log sources, potentially from multi-cloud environments, in a central location.

Once log collection has been configured, conducting research over time into baseline activities will help determine which events truly reflect something of concern. That being said, alerting and monitoring is only as helpful as those observing the data generated by these systems, as they are never fully autonomous.

Integrity

The app must have mechanisms in place to protect ePHI from improper alteration or destruction. Here too, a developer must consider how the ePHI is used on the platform and determine where the risk of alteration or destruction of ePHI might exist. Once those areas are identified, security measures must be implemented to reduce those risks.

Alerting and monitoring can also help preserve data integrity. At a minimum, the app should have some technical means for detecting changes to ePHI data. More sophisticated telehealth app developers will leverage privileged access management as an additional layer of security that protects ePHI integrity. PAM restricts access to administrator accounts or accounts that have broad rights to sensitive data to a select few individuals for a limited period of time.

Person or entity authentication

The Security Rule requires, where feasible, the system have a means of verifying the identity of the user, though the standard does not describe any implementation specifications. The use of passwords, PINs, tokens or biometrics are various technical means of meeting this requirement.

Due to the sensitive nature of ePHI that telehealth apps can store or exchange, any telehealth app should integrate a strong authentication workflow. Authentication is the process by which a user proves its identity to the app or its supporting infrastructure. Most apps rely on a combination of username and password, but those are often reused and/or simplistic. This leads to an increased risk of compromised authentication credentials.

Telehealth app developers should consider implementing multifactor authentication for both end users and employees or vendors. Other factors beyond username and password (something you know) could include app-based or text message codes (something you have) or biometric data, like fingerprints (something you are). This provides an extra layer of security protection that can mitigate the risk of a wide variety of types of attacks. MFA has experienced widespread use in other sectors, such as the financial sector, and telehealth apps should consider following suit.

The final standard is transmission security. App developers should consider the communication channels being used for transmitted ePHI and implement appropriate means of securing the transmission. In the current app ecosystem, both web and mobile apps that rely on server-based infrastructure require public-facing application programming interfaces to make the app's data available.

APIs are what enable apps to leverage or share data with third parties, such as when a user connects a social media account to an app to access photos or other data from a social media profile. Misconfigured or improperly-secured APIs have been the source of many breaches and require rigorous testing and auditing.

There are two implementation specifications for this standard.

Integrity control

Similar to the integrity standard, safeguards must be put in place to ensure that electronically transmitted ePHI is not improperly modified without detection. Cryptographically signing messages can help to detect modification of data.

Encryption

Similar to the access control standard, encryption technology must be utilized as appropriate to protect transmitted ePHI from unauthorized access by individuals or software programs. The Security Rule does not specify the use of any particular encryption standard. Rather, a developer should choose an encryption solution that appropriately addresses the security threat level presented by the transmission system being utilized.

Designing telehealth apps poses a number of unique challenges to developers, and the requirements of HIPAA's Security Rule is chief among them. Determining the best technical means for complying with HIPAA's standards requires judgment and expertise, as each application will demand a different set of solutions tailored to the app's uses and functionality. Inadequate or lax app design can result in poor app adoption and significant legal exposure. Consulting with the right legal and data security professionals as part of the development process ensures these critical issues are identified and addressed.

Photo by National Cancer Institute on Unsplash