Data Security in 2021

Unfairness, Deception, and Reasonable Measures

By John Rolecki and Yezi (Amy) Yan

ANDY/ISTOCK/GETTY IMAGES PLUS

In 1914, President Woodrow Wilson signed the Federal Trade Commission Act (FTCA).[1] At the time, the law—which, of course, established the Federal Trade Commission (FTC or Commission)—was intended to protect consumers from unfair, deceptive, and anticompetitive practices. In 2002, the FTC started to enforce the FTCA in a way that could not possibly have been foreseen in 1914: to regulate businesses' cybersecurity practices.

In 2021, privacy concerns are at the forefront of our national consciousness to a greater extent than ever before. On January 21, 2021, President Biden appointed Commissioner Rebecca Kelly Slaughter as the FTC's acting chair, signaling an aggressive approach to tech regulation. Indeed, within the last year, in prepared remarks, Slaughter endorsed "using [the FTC's] current authority fully and creatively, including by dusting off overlooked or under-utilized tools."[2] These included potentially expanding the Commission's use of the "unfairness" prong of section 5 of the FTCA—as opposed to the "deception" prong—more aggressively in the context of data security "because it sends a unique and important signal to the market separate from a deception count: Failure to take proper care of consumer data is illegal even if you do not lie about it."[3]

But what are the reasonable safeguards that inform whether a business takes proper care of consumer data in 2021? And how does the answer impact how we approach advising clients on related regulatory, litigation, and cyber insurance matters?

An understanding of the FTC's construct of "reasonable measures"[4] is tremendously valuable not only to facilitate compliance with the FTCA and various other federal statutes governing cybersecurity but also to properly evaluate cybersecurity-oriented issues in private litigation and—as the issuance of cyber insurance policies continues to rise—insurance underwriting and coverage issues.

First, we will explore the FTC's most recent positions on the issue to lay the foundation to understand this important standard. Then, we will explore how the impact of this standard goes beyond FTCA compliance alone. Finally, we will identify a few baseline measures that businesses can take to develop and maintain appropriate data security safeguards.

Lessons from FTC Enforcement Actions and Statements

The FTC derives its general authority to enforce privacy and cybersecurity standards from its mandate to protect consumers under section 5 of the FTCA. Specifically, section 5(a) prohibits "unfair or deceptive acts or practices in or affecting commerce."[5] A number of other federal statutes extend the FTC's reach to practices that would not otherwise fall under section 5(a), such as children's privacy, email marketing, and credit protections. These statutes essentially require the FTC to treat certain violations as if they were unfair or deceptive acts or practices under section 5(a).

After the FTC has filed an administrative complaint against the target of an investigation, which sets forth specific charges and is accompanied by a proposed settlement, the respondent may choose to either settle the charges or contest the complaint. The vast majority of respondents choose to settle. Typically, after several months of communications, the FTC and the respondent will enter into a proposed consent agreement, which will then be entered as a final enforceable consent order.

Though the consent orders do not require respondents to admit wrongdoing, together with the FTC's complaint they reveal the FTC's analysis of the respondent's allegedly wrongful acts and the negative consequences that stem from them. Consent decrees are posted publicly on the FTC's website, and, although the FTC's consent orders and complaints are not always the fountain of guidance we wish them to be, they frequently provide insight about what practices the FTC considers inappropriate. Several common themes have emerged.

Settlement with Zoom. No cybersecurity article during this time is complete without an assessment of the FTC's November 9, 2020, consent order with Zoom Video Communications, Inc.[6]

When the coronavirus outbreak prompted stay-at-home orders across the country and forced Americans to adapt to a new, socially distanced reality, Zoom soared in popularity and was thrust into the spotlight—alleged privacy and security lapses and all.

Zoom had been touting its use of "end-to-end encryption" in its marketing materials since as early as 2016. However, after much criticism, its chief product officer admitted in an April 2020 blog post that this was misleading. End-to-end encryption is a method of securing communications where an encrypted communication can only be deciphered by the communicating parties. Instead, Zoom employed "transport encryption," which encrypts the meetings but still allows the Zoom service to access the content of Zoom meetings.

The encryption issue was only the beginning of Zoom's cybersecurity controversies. Subsequent class actions filed against Zoom cited various issues, including vulnerabilities that allegedly allowed malicious actors to access users' webcams, the company's failure to stop "Zoom-bombing" incidents, and a data-mining feature that allowed some participants to surreptitiously access LinkedIn profile data about other users without notice or permission.

In May 2020, the FTC announced that it was looking into Zoom's privacy practices. Its subsequent complaint alleged, in part, that Zoom failed to implement adequate training programs on software development principles, failed to test and audit its applications for security vulnerabilities, and failed to monitor service providers and contractors with access to Zoom's server. The FTC also noted that Zoom was over a year behind in patching software in its commercial environment.

Zoom and the FTC entered into a settlement on November 9, 2020. The agency announced that "Zoom has agreed to a requirement to establish and implement a comprehensive security program, a prohibition on privacy and security misrepresentations, and other detailed and specific relief to protect its

TIP: In 2021, data security is a board-level issue and, as the FTC has increasingly signaled, should be treated as such.

user base."[7] As part of the information security program, Zoom must take specific measures aimed at addressing the problems identified in the complaint, such as undergoing yearly third-party audits of its security program.

Although the vast majority of FTC cases are resolved unanimously, in this instance two of the commissioners released dissents with suggestions that would aid both existing and emerging companies in enacting privacy programs that provide consumers with adequate security. Slaughter and Commissioner Rohit Chopra expressed concerns that the FTC's settlement did not do enough to protect the privacy of consumers.

Chopra challenged "[t]he FTC's status quo approach to privacy, security, and other data protection law violations" as "ineffective," arguing that

> investigations should seek to uncover how customers were baited by any deception, how a company gained from any misconduct, and the motivations for this behavior. . . . While deciding to resolve a matter through a settlement, regulators and enforcers must seek to help victims, take away gains, and fix underlying business incentives.[8]

He proposed issuing orders for consumers to be released from any contract lock-in with the company and imposing monetary penalties to further deter noncompliance.

Slaughter joined Chopra's dissenting statement, also opining that the FTC failed to properly appreciate and protect consumers' privacy. She explained: "Too often we treat data security and privacy as distinct concerns that can be separately preserved. In reality, protecting a consumer's privacy and providing strong data security are closely intertwined, and when we solve only for one we fail to secure either."[9]

The dissenting statements from Commissioners Slaughter and Chopra suggest that the FTC may place a greater emphasis on privacy violations in the future, rather than focusing exclusively on changes to companies' cybersecurity regimes.

John Rolecki *is a partner at Varnum LLP in Grand Rapids, Michigan. His practice focuses on counseling clients on data privacy and security matters, including with respect to connected and autonomous vehicles, as well as insurance coverage and commercial litigation. He may be reached at jjrolecki@varnumlaw.com.* **Yezi (Amy) Yan** *is an associate at Varnum LLP. She is a skilled researcher with experience in corporate, tax, and litigation matters. She may be reached at yeyan@varnumlaw.com.*

This is further underscored by the fact that President Biden has nominated Chopra to head the Consumer Financial Protection Bureau (CFPB) and, as noted above, appointed Slaughter as acting chair of the FTC.

Lessons learned from the Zoom settlement. Public commitments about data security are no place for puffery. Whenever a business commits to data security practices—including in privacy policies, where such representations have become customary, or even required—the business must do what it says it does.

Furthermore, the failure to disclose the existence of software during an install or upgrade process could trigger allegations of misrepresentation. Consumers should be made aware of any type of additional software being installed or left behind on their devices during an installation or upgrade process.

The Biden administration's appointment of Slaughter as acting chair of the FTC also signals the growing importance of taking measures to protect consumers' privacy; enforcement actions could arise even where a business has made no misrepresentations.

Proposed settlement concerning Ascension Data & Analytics. Although the case is not yet formally settled, the FTC's complaint and proposed settlement concerning Ascension Data & Analytics, LLC, provide further guidance for businesses reviewing their cybersecurity practices.[10]

Ascension is an analytics company that provides data, analytics, and technology products in connection with mortgages. Notably—and in stark contrast to the Zoom action—the FTC's allegations against Ascension had nothing to do with the adequacy of Ascension's *own* network, storage, or encryption practices. Rather, the FTC took issue with what it alleged was Ascension's failure to appropriately assess whether *its contracted service providers* could reasonably protect the personal information that Ascension disclosed to them. Furthermore, the FTC alleged that, based in part on Ascension's own representations in its privacy policy, the company was obligated to contractually require its service providers to implement appropriate safeguards for that personal information but failed to do so.

As a result, the FTC's proposed settlement provides a road map to establish reasonable measures to ensure that personal information that a business discloses to third-party service providers remains secure. Prior to sharing any protected information with any vendor, Ascension would be required to obtain from the vendor both (1) documentation regarding its information security policies and (2) a description of how and where Ascension's protected data will be maintained and safeguarded. The order also requires Ascension's vendors to have methods in place to assess the cybersecurity risk to its protected information on their networks, including annual vulnerability scanning and penetration testing. Further, after engaging any vendor, Ascension would be obligated to conduct an annual assessment of the vendor to determine the continued adequacy of its safeguards, similarly audit and test its own data security safeguards on an annual basis, identify and address risks

to the security of the provided information, and reevaluate on an annual basis the data security program that the order would also require Ascension to create and adhere to.

Like in the Zoom settlement, Chopra wrote a dissenting statement that lamented the FTC's failure to adequately provide redress for consumers or deter other firms from similar misconduct.[11]

Lessons learned from the Ascension proposed settlement. Here, the FTC's focus on the regulated entity's vendors highlights two principles underlying the concept of reasonable measures: (1) properly securing personal data includes proper diligence regarding any third-party relationship that involves data sales, sharing, or disclosure; and (2) again, businesses must live up to their own representations of how data they collect and control is secured—including downstream.

Settlement with Tapplock. Among the standard requirements listed in recent FTC orders, the May 18, 2020, settlement with Tapplock, Inc., provides further insight regarding the specific security measures that the FTC considers reasonable for a business that sells devices vulnerable to cyberattacks.[12]

Tapplock is a company that sells internet-connected, fingerprint-enabled padlocks (smart locks) to U.S. consumers. The locks interact with a companion mobile application that allows users to lock and unlock their smart locks when they are within Bluetooth range. This app logs usernames, email addresses, profile photos, location history, and the precise geolocation of a user's smart lock. Tapplock claimed to "follow industry best practices" to secure the locks from misuse or alteration.[13]

The FTC disagreed. It alleged that security researchers found at least three foreseeable security vulnerabilities with Tapplock's products—one of which allegedly permitted a person to easily lock and unlock any nearby smart locks—that could have been avoided with simple, low-cost steps. Further, despite Tapplock's representations otherwise, the FTC alleged that the company did not have any cybersecurity program for quite some time. This, the FTC alleged, led to the company's failure to employ sufficient security measures, which in turn led to the exposure of consumers' personal information.

Tapplock and the FTC reached a consent agreement on May 18, 2020. The agreement bars the company from misrepresenting the extent to which the company maintains and protects the security of personal information and the security of the devices at issue. It also requires Tapplock to implement technical measures to monitor its device networks for unauthorized activity and to establish data access controls, like access authentication and limitations for inbound connections and employee access, for all databases storing personal information. Notably, the consent order also requires the company to provide annual copies of these security programs, and any updates, to its board of directors or, if none exists, to a senior officer designated as responsible for the plan.

Lessons learned from the Tapplock settlement. Together, the Tapplock, Ascension, and Zoom orders—among others—provide an ongoing warning to businesses to thoughtfully and accurately represent their data security practices. Aside from the alleged misrepresentation aspect, Tapplock is additionally instructive in that it concerns device-oriented breaches and mandates engagement at the leadership level.

Businesses must live up to their own representations of how data they collect and control is secured—including downstream.

While the technical aspects underlying the required reasonable measures applicable to different devices will vary, the general steps would be the same: test the device for cyberattack risks and take actions accordingly, including those as simple as updating device control software. In 2021, cyberattacks should always be viewed as foreseeable, and compliance requires constant vigilance.

Settlement with SkyMed. The FTC's February 5, 2021, settlement with SkyMed International, Inc., further reinforces what the FTC considers fundamental reasonable cybersecurity measures that are applicable to any business.[14]

SkyMed is a Nevada-based company that provides travel emergency services. The FTC alleged that, in the course of completing membership applications, SkyMed required applicants to submit detailed health information and provide SkyMed access to the applicants' medical records. The FTC alleged that, after obtaining this information, SkyMed "engaged in a number of practices that *failed to provide reasonable security* for the personal information it collected," including failing to develop adequate written information security policies, failing to adequately train employees and contractors, and maintaining consumer data for longer than necessary.[15] The FTC also noted that SkyMed failed to monitor for unauthorized attempts by third parties to exfiltrate personal information.

The settlement agreement, which the FTC approved in February 2021, includes specific requirements to rectify the alleged lack of reasonable security. This includes implementing procedures for systematically inventorying personal information in the company's control, deleting personal information that is no longer necessary, encrypting sensitive personal

information, training employees, and increased monitoring and data access controls for repositories of personal information. Like the Tapplock settlement, these measures also require the company to provide annual copies of the security plan to its board or designated senior officer.

Lessons learned from the SkyMed settlement. The lesson of SkyMed is that, within the last year, the FTC both expressly labeled the specific allegations above as less than reasonable measures and prescribed specific, replicable measures to remedy these types of shortcomings. Perhaps more than in any other recent case, the FTC's settlement with SkyMed may be taken as valuable guidance of fundamental requirements for companies controlling sensitive personal information—including elevating cybersecurity issues to a leadership-level priority.

An organization should have clear accountability for cybersecurity at its highest levels.

Settlement with Equifax. The FTC's July 2019 settlement with Equifax, which relates to the alleged practices leading to one of the largest breach events in U.S. history, contains ongoing lessons about basic actions that are likely to be considered reasonable data security measures.[16]

In a nutshell, in March 2017, US-CERT—Homeland Security's cyber experts—alerted Equifax about a critical security vulnerability in a certain open-source software. The alert warned anyone using a vulnerable version of the software to update it immediately to a free patched version. The press soon reported that hackers had already started to exploit the vulnerability. Equifax, however, allegedly neglected to forward this alert to the appropriate network staff and failed to utilize network monitoring equipment capable of detecting the type of intrusion at issue. Making matters worse, because Equifax's databases were not segmented, vast amounts of information could be exposed based on just one breach point.

Among other things, the FTC's consent order in this matter has a particular focus on patch management and network monitoring. Specifically, the order contains two sections devoted to requiring that Equifax (1) establishes patch management policies and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed, and (2) establishes and enforces policies and procedures to ensure the timely remediation of critical and/or high-risk security vulnerabilities. The FTC also required Equifax to document and identify its IT asset inventory, limit unauthorized access by segmentation of network and databases, develop and implement intrusion protections, and provide annual employee training on data security awareness.

Lessons learned from the Equifax settlement. There are three ready takeaways from the sprawling Equifax story as to reasonable data security measures: (1) patch your software, (2) segment your network, and (3) monitor for intruders.

Settlement with DealerBuilt. Finally, the FTC's June 2019 settlement of its enforcement action against LightYear Dealer Technologies, LLC, provides additional guidance for businesses regarding data security accountability and planning.[17]

LightYear Dealer Technologies, LLC, doing business as DealerBuilt, offers an automotive dealer management system that is used nationwide. The system is designed to collect and maintain large quantities of personal and competitively sensitive information relating to both consumers and employees. The FTC alleged that DealerBuilt collected and stored this information with no access controls or authentication protections, such as passwords or tokens.

Like most respondents to an FTC complaint, DealerBuilt chose to settle. Similar to the other consent orders discussed in this article, the FTC required DealerBuilt to develop, implement, maintain, and document an information security program and obtain regular third-party security assessments. Again, however, it is worth noting that the FTC also required DealerBuilt to provide annual copies of the security plan and any updates to its board of directors or, if none exists, to a senior officer designated as responsible for the plan.

Lessons learned from the DealerBuilt settlement. In prepared remarks delivered in October 2020, Slaughter identified this case as exemplifying, at least in part, the principle of unfairness, as opposed to deception: "[f]ailing to implement necessary safeguards is unfair, and using or sharing data beyond what a reasonable consumer would expect is unfair."[18]

The DealerBuilt settlement further underscores the FTC's stance—espoused by Slaughter—that cybersecurity is a board- and/or senior officer–level issue. As noted above, this requirement also appeared more recently in the FTC's Tapplock and SkyMed settlements. An organization should, therefore, have clear accountability for the issue at its highest levels. Documenting regular, affirmative actions taken by organizational leadership to assess and manage the issue is encouraged.

FTC Guidance: Valuable beyond FTCA Compliance

Compliance with the FTCA—and other federal statutes containing data security elements, such as the Health Insurance Portability and Accountability Act (HIPAA), the

Gramm-Leach-Bliley Act (GLBA), the Children's Online Privacy Protection Act (COPPA), and others—is important, and the FTC has signaled continued aggressive enforcement in the data security context. But these guideposts for the meaning of "reasonable measures" for cybersecurity inform a host of issues arising in private litigation as well.

Website privacy policies. First, to the extent that businesses represent that they have implemented reasonable cybersecurity measures to protect personal information collected through a website—for instance, in website privacy policies, where this is becoming a customary, or even required, representation—the FTC's current and future positions will inform the standard applied in any private litigation over those specific representations in the event of a data breach. Causes of action frequently appearing in these types of lawsuits include breach of contract and a number of common-law privacy torts. Several highly publicized lawsuits remain ongoing at this time, with more certain to arise over the course of 2021.

For instance, in *In re Hanna Andersson & Salesforce.com Data Breach Litigation*, which at this writing remains pending in the U.S. District Court for the Northern District of California, consumers alleged that the defendants violated the California Consumer Privacy Act (CCPA) by not doing enough to protect from hackers the personal information of over 100 class members.[19]

In *In re Marriott International, Inc., Customer Data Security Breach Litigation*, pending in the U.S. District Court for the Southern District of Maryland, plaintiffs alleged that Marriott conducted inadequate due diligence in the course of acquiring Starwood.[20] This led to the persistence of several vulnerabilities in the acquired business's system, which, the plaintiffs alleged, Marriott failed to appropriately address. Notably, the plaintiffs expressly asserted that the FTC's action against Equifax "was another red flag" for Marriott in that the alleged deficiencies in that FTC action were "strikingly similar" to the alleged deficiencies identified by the Marriott plaintiffs. These included (1) running obsolete or outdated software, (2) a failure to implement a process to ensure that software was updated and patched, (3) a failure to implement adequate encryption, (4) a failure to implement adequate authentication measures, (5) a failure to adequately monitor its system for breaches, and (6) a failure on the part of senior management to create the appropriate culture around data security. This express incorporation of the FTC's prior expression of what constitutes reasonable measures—or not—makes clear the strong effect that the settlements above, and those to come, have on determining the standard for reasonable measures in various forums nationwide.

CCPA private right of action. Second—and relatedly—as readers active in the data privacy space are well aware, the CCPA created a private right of action for consumers whose data was subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices."[21] Although this language is particular to the CCPA, as the Marriott litigation demonstrates, its interpretation will doubtless be informed by the FTC's current and future positions.

State-specific data security obligations. Third, all 50 states have laws governing data breach events, and several impose an obligation to take reasonable measures to protect and secure personal information. Even where a private right of action does not exist, state attorneys general are frequently authorized to initiate lawsuits against companies allegedly failing to comply with these statutory data security obligations. Although, as with the CCPA, these state-specific statutes will likely develop their own nuances, the FTC activity in the area will almost certainly be a lodestar for overall development of the notion of reasonable data security practices.

Cyber insurance. Finally—for this article, at least—the FTC's activity in this area is, and will continue to be, instructive to the underwriting and operation of cyber-risk insurance policies. On the front end, a business's ability to demonstrate ongoing compliance with industry best practices will almost certainly reduce premium costs. Further, however, to the extent that a cyber policy contains exclusions relevant to these standards—for instance, a contractual liability exclusion that could be keyed to claims potentially made in private litigation, as suggested above—the extent to which businesses can demonstrate the implementation and maintenance of reasonable cybersecurity measures under applicable law could be a primary battleground in determining the extent of coverage available for costly data breach attacks.

What Businesses Can (and Should) Do

Although we cannot prescribe a foolproof, one-size-fits-all approach to cybersecurity in this article, we can identify fundamental principles that, according to the FTC's recent statements, will be useful in advising clients in these matters.

Make a plan (and stick to it). Due largely to unfortunate, large-scale cybercrime, the topic of cybersecurity is more prominent than ever. Beyond representations (hopefully not buried) in privacy policies, now more than ever before privacy is a marketable brand. Be aware, however, that when security-oriented representations are made, they must be implemented, achieved, and maintained. As several of the FTC opinions explored above make clear, this cannot be done correctly without a clearly articulated and documented plan specifically oriented to the business involved—both in terms of establishing reasonable security measures and breach-response procedures. Notably, the FTC clearly disapproves of a "set it and forget it" approach to data security. Once formed, a data security plan should be audited, tested, and, if necessary, revised on an annual basis.

Designate a point person in leadership. As the FTC has indicated through its DealerBuilt, SkyMed, and Tapplock settlements, it is a good idea to integrate board- and/or officer-level responsibility for audit, review, and response tasks. Notably, Slaughter recently identified "a threshold inquiry

that [the FTC] should make in all cases: Our investigations should include questions to determine the involvement of senior leaders in the alleged wrongdoing and the internal compliance culture that allowed the wrongdoing to occur."[22]

Once formed, a data security plan should be audited, tested, and, if necessary, revised on an annual basis.

Moreover, in responding to a cybersecurity event, speed matters. The optimal time to work through organizational authority and accountability is not in the midst of an unauthorized breach. Leadership and preparedness play a key role in an effective response. Don't forget to involve insurers (and attorneys) at an early stage. When one person—or committee—is formally tasked with implementing a preparedness and response plan, the various moving parts are less likely to fall through the cracks.

Rely on experts. Cyberattacks come in various forms and levels of sophistication. Do not, however, assume that because a business is small or midsize it will probably only be subject to attacks of middling sophistication. No business is too small to suffer a clever, devastating attack. Establish a relationship with cybersecurity consultants who can help organizations of any size design, audit, and test security measures. These consultants are also invaluable when the time comes to assess and respond to a security incident, not only in the moment, but also to inform the business's legal obligations, if any, following an incident.

Encrypt, segment, and restrict access. The FTC has made clear that the manner in which personal data is stored bears on its assessment of whether the protective measures are reasonable or not. Encrypting data (and holding the encryption key separately from the encrypted information); keeping sensitive personal data separate from general data; and keeping such data on a restricted, need-to-know basis within an organization are relatively simple steps that can significantly mitigate a business's risk. Building on the prior points, industry experts can readily expand on the foregoing and undertake the testing and maintenance required to implement and maintain an appropriate data security plan.

Integrate fair information practice principles. Slaughter's recent comments cited herein underscore the importance of considering relevant fair information practice principles (FIPPs) in the context of any cybersecurity assessment. The FTC's SkyMed decision, for instance, highlights the importance of understanding what personal information a business possesses, the purposes for which the information was collected, and whether the purpose for maintaining that personal information continues to be served. Where there is no reason to retain data, delete it—particularly when it no longer serves the purpose for which it was collected. Cybercriminals cannot access what a business does not possess.

Conclusion

It is difficult to imagine 2021 being anything other than an eventful year in cybersecurity. The challenges that businesses face in protecting the sensitive personal data they control will continue to grow. In turn, statutory and common-law standards employed to enforce these obligations will continue to develop. As the concepts of unfairness, deception, and reasonable measures become increasingly particularized over time, it is well worth paying close attention to and learning from the trials of others. ◄

Notes

1. 15 U.S.C. §§ 41–58.
2. Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, Remarks at the New York University School of Law Cybersecurity and Data Privacy Conference: FTC Data Privacy Enforcement: A Time of Change 5 (Oct. 16, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581786/slaughter_-_remarks_on_ftc_data_privacy_enforcement_-_a_time_of_change.pdf.
3. *Id*.
4. *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); *see also* Fed. Trade Comm'n, Start with Security: A Guide for Business (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.
5. 15 U.S.C. § 45(a).
6. Zoom Video Commc'ns, Inc., File No. 1923167 (F.T.C. Nov. 9, 2020) (agreement containing consent order), https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf.
7. Press Release, Fed. Trade Comm'n, FTC Requires Zoom to Enhance Its Security Practices as Part of Settlement (Nov. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.
8. Dissenting Statement of Commissioner Rohit Chopra, *Zoom Video Commc'ns*, File No. 1923167, at 2, 4 (F.T.C. Nov. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1582914/final_commissioner_chopra_dissenting_statement_on_zoom.pdf.
9. Dissenting Statement of Commissioner Rebecca Kelly Slaughter, *Zoom Video Commc'ns*, File No. 1923167, at 3 (F.T.C.

Nov. 9, 2020), https://www.ftc.gov/system/files/documents/public_statements/1582918/1923167zoomslaughterstatement.pdf.

10. Ascension Data & Analytics, LLC, File No. 1923126 (F.T.C. Dec. 15, 2020) (complaint), https://www.ftc.gov/system/files/documents/cases/1923126ascensioncomplaint.pdf; Ascension Data & Analytics, LLC, File No. 1923126 (F.T.C. Dec. 15, 2020) (agreement containing consent order), https://www.ftc.gov/system/files/documents/cases/1923126ascensionacco.pdf.

11. Dissenting Statement of Commissioner Rohit Chopra, *Ascension Data & Analytics*, File No. 1923126 (F.T.C. Dec. 14, 2020), https://www.ftc.gov/system/files/documents/public_statements/1584706/final_chopra_statement_on_ascension_redacted.pdf.

12. Tapplock, Inc., File No. 1923011 (F.T.C. May 18, 2020) (decision and order), https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockorder.pdf.

13. Tapplock, Inc., File No. 1923011 (F.T.C. May 18, 2020) (complaint), https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockcomplaint.pdf.

14. Press Release, Fed. Trade Comm'n, FTC Gives Final Approval to Settlement with Emergency Travel Services Provider Related to Allegations It Failed to Secure Sensitive Data (Feb. 5, 2021), https://www.ftc.gov/news-events/press-releases/2021/02/ftc-gives-final-approval-settlement-emergency-travel-services.

15. SkyMed Int'l, Inc., File No. 1923140 (F.T.C. Dec. 16, 2020) (complaint) (emphasis added), https://www.ftc.gov/system/files/documents/cases/skymed_-_complaint.pdf.

16. Press Release, Fed. Trade Comm'n, 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; *see* Fed. Trade Comm'n v. Equifax Inc., No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019) (stipulated order for permanent injunction and monetary judgment), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf.

17. LightYear Dealer Techs., LLC, File No. 1723051 (F.T.C. June 12, 2019) (decision and order), https://www.ftc.gov/system/files/documents/cases/172_3051_dealerbuilt_decision_order.pdf.

18. Slaughter, *supra* note 2, at 5 (footnote omitted).

19. No. 3:20-cv-00812-EMC (N.D. Cal. Dec. 29, 2020) (proposed settlement).

20. MDL No. 19-md-2879 (S.D. Md. Oct. 26, 2020) (memorandum opinion).

21. Cal. Civ. Code § 1798.150.

22. Slaughter, *supra* note 2, at 3.