Antitrust, Vol. 34, No. 3, Summer 2020.

The *Other* Tech-Focused Initiative: The FTC's Expanding Consumer Protection Efforts Targeting E-Commerce

BY RICHARD CUNNINGHAM, OLIVIA ADENDORFF, LUCIE DUVALL, AND RACHAEL REZABEK

WITH MUCH FANFARE, THE U.S. Department of Justice and U.S. Federal Trade Commission have each launched major initiatives to evaluate the application of the antitrust laws to the conduct and deal activity of major technology firms. The DOJ has created a task force reporting directly to the Attorney General.[1] The FTC has created an entirely new Technology Enforcement Division and initiated a retrospective study under its Section 6(b) authority.[2] What will come of these initiatives remains to be seen.

This article focuses on an equally significant—but much more subtle, incremental, and long-term—investment by the FTC in consumer protection enforcement in this same sector. As discussed below, there are several important areas of significant recent change and ongoing ambiguity in the Commission's expansive enforcement program relating to e-commerce and technology, including issues relating to disclosure standards, data security practices, and privacy.

We began work on this article before the COVID-19 mitigation efforts upended commerce and our way of life earlier this year, with the expectation that the upcoming election would be the primary event impacting FTC enforcement.

Richard Cunningham and Olivia Adendorff are partners, and Lucie Duvall and Rachael Rezabek are associates, at Kirkland & Ellis LLP in Washington, DC and Dallas, TX. Mr. Cunningham served as Staff Attorney and Senior Trial Counsel with the FTC Bureau of Competition from 2004 to 2013. The authors have represented, or are representing, several of the companies involved in the matters or issues discussed below, including DirecTV, Facebook, LendingClub, and clients whose involvement or representation is nonpublic.

While the effects of this unprecedented situation on our economy will not be fully visible for some time, it appears that a significant expansion of consumers' use of e-commerce has occurred. It is hard to envision this shift or the other implications of the COVID-19 situation diminishing the FTC Bureau of Consumer Protection's focus on the technology sector. It is likewise hard to imagine that the 2020 election will lead to a reduction in the attention the FTC directs to enforcing the consumer protection laws in this space—the agency is very active in this technology and e-commerce during the current Republican administration, and the Democratic FTC Commissioners Rohit Chopra and Rebecca Slaughter have been calling for even more expansive and aggressive enforcement.[3] Thus, scrutiny of technology and e-commerce ranging across the entirety of the Bureau of Consumer Protection's mission is likely to continue.

Advertising Disclosures

The FTC in 2000 issued, and in 2013 revised, its ".com Disclosures," a guidance document discussing the applicability of consumer protection laws to online marketing.[4] These guidelines state that online advertisers have the same legal obligation as print and television advertisers to ensure that disclosures are "clear and conspicuous." But despite the FTC's devoting several dozen pages to the issue, exactly what makes an online disclosure clear and conspicuous is less black and white than one might expect, as illustrated by *FTC v. DirecTV*.

In *DirecTV*, the FTC sought a nearly $4 billion monetary remedy in connection with claims that the company failed to adequately disclose certain terms of purchase for its satellite television service.[5] The FTC challenged DirecTV's print advertisements as "tout[ing]" an "eye-catching $19.99 monthly rate for twelve months without clearly explaining that" consumers were signing a two-year commitment, that the introductory rate would end after the first year, or that consumers would be charged a fee for early cancellation.[6] The FTC further asserted that DirecTV's online disclosures were deficient because, among other things, DirecTV failed to adequately disclose that it would bill consumers for premium channels "unless consumers took the affirmative step of canceling" before the free introductory offer period ended,[7] and because certain key terms of the subscription service were presented (in at least one version of the website) through hyperlinks, info hovers, and tool tips.[8] At trial, upon the conclusion of the FTC's case in chief, the court expressed doubts that the FTC had met its burden of proof. The court then suspended the trial and roughly a year later dismissed the portion of the case relating to DirecTV's print advertisements.[9] The FTC subsequently abandoned its remaining online disclosure claims, apparently recognizing that there was a significant likelihood that the court would find DirecTV's online disclosures compliant. The dismissal eliminated the possibility of a judicial ruling addressing the application of the clear and conspicuous standard in the online environment.

DirecTV suggests that there may be a material gap between the FTC's interpretation of the required disclosures in an online context and the interpretation that will be enforced by at least some courts, and creates significant ambiguity regarding the disclosure standards applicable to e-commerce sales and marketing. To date, to our knowledge, the FTC has said virtually nothing regarding the implications of the *DirecTV* decision and the agency's subsequent decision to dismiss the remainder of the case.[10]

Other litigated FTC cases provide little information regarding whether the FTC's approach to the clear and conspicuous standard in the context of online disclosure is (or will be) accepted by courts. In general, past FTC actions involving e-commerce disclosures have challenged obviously deficient (or nonexistent) disclosures and/or have concerned scams, and thus do not illuminate the line between adequate and inadequate disclosures. For instance, *FTC v. Cyberspace.com* involved what appeared to be "a check, usually for $3.50" addressed to the recipient that also had "small print disclosures" on the back "revealing that cashing or depositing the check would constitute agreement to pay a monthly fee for internet access" that would be billed through the recipient's monthly phone bill. The case was decided and affirmed on summary judgment because the communication "create[d] an overall impression that the check resolves some small outstanding debt" rather than creating a contract to acquire internet services.[11] Similarly, *FTC v. Grant Connect* addressed disclosures that were, in the words of the court, "buried by the larger, sensationalized text regarding the amount of credit, the zero percent interest, and the images of a traditional credit card."[12] These fact patterns are so clearly noncompliant that they do not provide much guidance regarding the standards for sufficient disclosure and did not warrant detailed discussion and analysis delineating compliant versus noncompliant disclosures by the fact finder.

The FTC's recent informal proceedings confirm rather than remedy the lack of clarity. In September 2016, the FTC hosted a workshop titled "Putting Disclosures to the Test," in which the FTC explored testing and survey methods that companies can use to evaluate the effectiveness of advertising disclosures.[13] In that workshop, a number of panelists presented information on different types of testing available to companies to help them understand whether their disclosures are seen and understood by consumers, ranging from mall intercept studies and small-scale qualitative studies to lab and eye tracking studies.[14] But implicit in the need to test disclosures is the absence of consensus regarding the criteria that would render disclosures legally compliant. For many companies, testing advertising disclosures may be unrealistic due to the cost and time involved; hence, the recommendation to test various disclosure strategies to determine their adequacy is often impractical.

In June 2019, the agency held a workshop entitled "That's the Ticket" focusing on covered disclosures relating to online ticket sales. A key topic addressed during the workshop was drip pricing,[15] a practice in which fees or charges added to the advertised price are disclosed several steps into the purchase process. To date, the FTC has issued a warning to hotel operators that the practice "may" be deceptive but has not pursued any enforcement actions.[16] FTC Commissioner Rebecca Slaughter has since commented on the "prisoner's dilemma" e-commerce merchants face when operating in a sector in which drip pricing is common: "If just one seller moves to all-in pricing, it may lose business to sellers who continue to hide the ball."[17]

Further elucidation of these issues is needed. It has been seven years since the .com Disclosures were last updated. Consumers increasingly engage in e-commerce using mobile devices, which come in a very broad range of screen sizes and formats. Varying ad formats continue to proliferate and increasingly complex transactions are occurring online, including the sale of financial products and real estate. Particularly in light of the *DirectTV* matter suggesting that disclosures that the FTC may not believe are clear and conspicuous under the .com Disclosures can in fact be legally compliant, gray areas abound. The FTC recently solicited research on topics relating to online marketing, including "[l]egal barriers to online marketing," the "differences between offline and online marketing," and the "distinct features of social media marketing."[18] The results of this outreach will be presented at an FTC conference on marketing and consumer protection currently scheduled for October 2, 2020. Such solicitations often precede industry guidance. Further discussion and examples from the Commission—in the form of an update or supplement to the .com Disclosures or in some other form—would assist e-commerce companies' compliance efforts.

Alternative Business Models

From streaming video to meal kits to stylist-selected clothing boxes, subscription-based business models have proliferated online. According to a 2018 study by McKinsey, the subscription e-commerce market grew by more than 100 percent annually from 2013 to 2018.[19] The success of a wide variety of e-commerce based subscription services suggests strong consumer demand for and acceptance of these services.

The FTC has long been skeptical of negative option marketing,[20] a common feature of subscription services, in which a seller interprets a consumer's failure to take an affirmative action as consent to be charged for a product or service. The FTC enforces the Restore Online Shoppers' Confidence Act (ROSCA), legislation signed into law in 2010, which provides the FTC with authority to draft and enforce rules applicable to online subscription services, including such services utilizing negative option structures.[21]

Unsurprisingly, in recent years, the FTC has focused its enforcement in this area almost entirely on e-commerce services. For example, in December 2017, the FTC entered into a $1.38 million settlement with AdoreMe, a subscription-based online lingerie and swimwear company, over allegedly

The fundamental premise of most of the Commission's actions . . . is that companies have an obligation to reasonably monitor the security of their databases, platforms, and networks, and take prompt and effective remedial action when issues arise.

deceptive claims surrounding the terms of its subscription-based service.[22] In addition, the FTC complaint also alleged that the company violated ROSCA by making it inordinately difficult for customers to cancel their subscriptions, including by forcing customers to cancel by telephone only.[23] In September 2019, the Commission sued AH Media Group for operating an online subscription program marketing "free trials" of cosmetics and dietary supplements to consumers, which allegedly required them to pay only $4.99 in shipping costs.[24] In reality, the FTC alleged, AH Media charged consumers roughly $90 for the products several weeks later and enrolled them without their knowledge in subscription plans for another substantial monthly fee. The FTC also alleged that the company made it extremely difficult for consumers to cancel their subscriptions in violation of ROSCA. The FTC has pursued similar enforcement actions against many other e-commerce companies advertising free trial offers for failing to adequately disclose the automatic conversion to paid subscriptions and/or the steps necessary to cancel.[25]

In September 2019, the Commission announced an initiative to revamp its existing negative option regulations, including the Negative Option Rule. We fully expect this process to lead to both heightened standards for compliance and more aggressive enforcement activity. For example, the Negative Option Rule currently addresses only pre-notification plans, a transaction structure in which a seller notifies its customers of the contents of their next shipment and the customers have a certain amount of time to reject the delivery.[26] The FTC's press release announcing the initiative described "whether the agency should use its rulemaking authority under the FTC Act to expand the scope and coverage of the existing Negative Option Rule" as an issue under consideration.[27] We read the omission of the words "or contract" after the word "expand" as a signal that expansion is likely.

In light of the success and prominence of many e-commerce subscription services, consumers likely have a higher baseline understanding of these business models than has existed in the past, and streamlined disclosures using features such as hyperlinks and tool tips may be sufficient in some instances to avoid misunderstanding of the service's structure and terms. The possibility of chilling innovation and practices consumers value through draconian disclosure requirements is a real risk in this area. For example, many consumers use and value free trial offers, but prescriptive disclosure or cancellation mechanism requirements could spur companies to promote their offerings in other ways that provide less value to consumers.

Data Security and Fraud Prevention

The FTC's growing and evolving data security enforcement program lacks a close pre-internet era analogue. The fundamental premise of most of the Commission's actions in this area is that companies have an obligation to reasonably monitor the security of their databases, platforms, and networks, and take prompt and effective remedial action when issues arise. The FTC typically invokes its authority to challenge "unfair" practices under Section 5 of the FTC Act to police data security practices, but the agency will also scrutinize a company's security- and fraud-related statements to identify representations that could serve as the basis of a deception theory. A key issue of ongoing uncertainty is exactly what a company must do pursuant to the FTC Act to protect its data or platform from third-party fraud, that is, what conduct is "reasonable" versus unreasonable.

FTC v. Wyndham Worldwide Corp. in 2015 was the first data security enforcement action to be litigated instead of resolved by pre-litigation settlement and remains a landmark case in this area. In *Wyndham*, the FTC alleged that the company's data security practices were unfair, asserting, among other things, that the company falsely touted "industry standard [security] practices."[28] Wyndham contended that it had been previously found PCI-compliant and, through a motion to dismiss, Wyndham (1) challenged the FTC's power to bring charges against private companies for their data security practices as "unfair" practices under Section 5 of the FTC Act; and (2) argued that the FTC's enforcement regime created constitutional vagueness problems because it was not grounded in clearly defined enforcement standards (an argument that, as explained below, would later be embraced by the Eleventh Circuit in the related context of scope of relief). In a 2015 ruling, the Third Circuit held that the FTC's unfairness authority is expansive, and that data security practices could be deemed "unfair" within the meaning of Section 5 of the FTC Act.[29]

In *FTC v. LabMD*, decided three years after the Third Circuit's decision in Wyndham, the Eleventh Circuit expressed significant discomfort with the lack of clear standards separating compliant data security practices from "unfair" ones.[30] In *LabMD*, the Commission initiated an administrative challenge in 2013 against a diagnostic laboratory for failing to provide "reasonable and appropriate" security for consumers' data, leading to the exposure of thousands of patients' personal information via a peer-to-peer file sharing network in violation of the unfairness prong of Section 5 of the FTC Act.[31] After an Administrative Law Judge dismissed the complaint in 2015, concluding that the FTC had failed to prove that LabMD's conduct had "caused or [was]

likely to cause substantial injury to consumers,"[32] the Commission issued an order in 2016 reversing the decision and requiring LabMD to create a "comprehensive information security program."[33] LabMD then challenged the order, contending (among other things) that the FTC did not have authority to regulate companies' data security practices—the exact issue that the Third Circuit had decided in the Commission's favor in the 2015 *Wyndham* decision. On appeal in 2018, the Eleventh Circuit declined to address whether the FTC had such authority, thereby avoiding a potential circuit split, but nonetheless declared the Commission's order against LabMD—which "command[ed] LabMD to overhaul and replace its data-security program" but contained no specific prohibitions—to be overly vague and thus unenforceable, as it required the company's data security program "to meet an indeterminable standard of reasonableness."[34]

In the wake of *LabMD*, the Commission has continued pursuing data security matters using slightly more detailed enforcement orders.[35] The 2019 FTC/Equifax settlement, a matter brought with the Consumer Financial Protection Bureau and 50 state attorneys and involving a $575 million dollar monetary remedy, reflects the Commission's current approach. The consent order requires Equifax to conduct annual assessments of security risks, implement appropriate safeguards to address those risks, test and monitor the effectiveness of such safeguards, and conduct third-party assessments of its information security program on a biennial basis, among other things.[36] Whether and in what context(s) some or all of these practices are necessary to avoid violating Section 5 in the first place is unclear.

Additional litigated cases would shed light on the standards a company must meet to avoid data security and fraud prevention practices that violate Section 5. In the meantime, however, this area involves a healthy dose of "I know it when I see it" prosecutorial discretion. But, because most Commission cases involve "red flags," either in the form of internal or external warnings[37] or clear overstatements of the level of security provided,[38] the absence of clear standards in this area has not yet led to large numbers of litigated matters. Should the Commission shift its enforcement efforts towards closer-to-the-line conduct, as often occurs as enforcement in a given area matures, clarity through formal guidance or some other means regarding exactly what practices are sufficient would become much more important.

Matters involving allegations that platform owners have inadequately policed and/or prevented fraud appears to be one area in which the Commission is pushing the envelope of its unfairness authority. In December 2019, the FTC and the State of Ohio obtained a temporary restraining order against Globex Telecom, Inc. for allegedly assisting and facilitating telemarketers that it knew (or consciously avoided knowing) were violating the Telemarketing Sales Rule (TSR), which prohibits calls delivering prerecorded messages.[39] As an extension of this effort, in January of this year, FTC Staff issued letters to 19 other VoIP service providers informing them of their duties under the FTC Act and Telemarketing Sales Rule to refrain from assisting and facilitating callers engaged in illegal telemarketing or robocalling.[40] The FTC sent similar letters to three additional VoIP providers on April 3, 2020, regarding the potential facilitation of COVID-19-related scams.[41] In addition, in 2019 the FTC sued the parent company of several online dating services for allegedly maintaining inadequate practices to prevent scammers from accessing its platforms, notwithstanding efforts to prevent such access.[42] Further activity in this area may spur the FTC and the courts to more clearly define and articulate the fraud-prevention practices companies should employ to avoid "unfair" conduct that violates Section 5.

Protecting Children

Another key FTC concern in e-commerce is the protection of children. This year marks the 20-year anniversary of the rule implementing the Children's Online Privacy Protection Act (COPPA)[43]—one of the first laws crafted at the advent of the dot-com era to respond to the technological innovations of the internet. But despite 20 years of FTC enforcement, 2019 represented a near sea change in the FTC's enforcement of the statute, with the FTC changing the order of magnitude of its monetary penalties. Early in the year the FTC obtained the largest civil penalty to date for a COPPA violation, from TikTok, of $5.7 million. Only six months later, in September 2019, the agency obtained a settlement nearly 30 times larger—$170 million—from YouTube.[44] The FTC did not in its public statements tie either penalty to a clear formula or methodology. The basis for the dramatic escalation in penalties, however, could—and in our view should—be made more transparent.

As to TikTok, the FTC alleged that the company's viral video app, failed to adequately secure consent from parents for collecting personal information from users under the age of 13. According to the FTC, TikTok operated for three years without asking users' ages, and then, after changing its practices, never retroactively obtained that information for legacy users. In its blog post discussing the settlement, the FTC focused on the substantive reach of COPPA: "Whether a company intends—or doesn't intend—to have a site directed to kids isn't what controls the [COPPA] analysis. Instead, the FTC will look to the site's look and feel, as well as evidence that the company had actual knowledge that users are under thirteen."[45] Neither the blog post nor the other materials surrounding the settlement explained how the FTC determined the civil penalty amount specified in the settlement.

In *YouTube*, the FTC alleged that that the company had actual knowledge of child-directed "channels" on its primary platform but did not seek to secure parental consent for the collection of personal information from children viewing these channels. The settlement requires YouTube to notify channel owners of COPPA's requirements and create a system

for channel owners to designate content as aimed at children, if appropriate. These requirements prompted YouTube to shift its business practices, including to use machine learning to proactively identify children's videos, require content owners to inform YouTube if content is directed at children, and cease serving personalized ads alongside child-directed content.[46] Neither the FTC's press release nor the consent order explain how the $170 million civil penalty was determined, but the Commissioner statements provide some insights into the calculation. The Statement of Chairman Simons and Commissioner Wilson stated that the penalty is "higher than" YouTube's "ill-gotten gains," and that the amount was determined by reference to "an analysis of the civil penalty factors set forth in Section 5(m) of the FTC Act: the degree of culpability; any history of similar prior conduct; ability to pay; effect on ability to continue to do business; and such other matters as justice may require."[47] Commissioner Chopra's Statement calls into question whether the Commission's calculation of YouTube's gains was complete, and suggests that an alternative assessment of such gains would yield a figure at least five times larger, exceeding a "billion" dollars.[48] Collectively, these statements indicate that YouTube's "gains" derived from the COPPA violation were a key input into its civil penalty calculations, there is *a broad* array of discretion and variability in how such gains are determined, and other unstated considerations also apply.

Whether through litigation, guidance, or a statement accompanying a future settlement, the Commission's approach to determining civil penalties in COPPA matters could be made much less opaque. Such transparency would benefit both the Commission and companies and individuals operating online, including by expediting future Commission settlement negotiations and arming individuals with compliance responsibilities with a significantly greater ability to concretely quantify COPPA exposure to decision-making executives.

Privacy and Information Sharing

One of the most important developments in the e-commerce space over the last decade is that the FTC has become a—if not the—leading privacy regulator in the United States. To date, the FTC's legal authority has been premised primarily on its authority to prohibit "deceptive acts or practices" under Section 5 of the FTC Act. While privacy practices probably were not what Congress had in mind in 1914 when enacting the FTC Act, the FTC has pursued dozens of enforcement actions (all resulting in settlements) premised on a theory that the defendant company misrepresented or failed to disclose its data or privacy practices to users.[49] The Commission has issued several statements and policy guidance documents setting forth its views on privacy, including public statements by the commissioners made in a number of privacy-focused congressional hearings.[50] In 2019, the Commission also filed a public comment on the widely-used National Institute of Standards and Technology (NIST) proposed privacy framework, which provides many companies guidance on seeking to manage privacy risks.[51]

While the Commission has yet to litigate a privacy case, in 2019, the recently finalized order enforcement settlement with Facebook broke the mold of prior Commission practice in this arena.[52] Through the settlement (which was approved by the district court in late April), Facebook agreed to pay $5 billion to resolve the FTC's allegations. This civil penalty is the largest fine ever imposed by the FTC and the largest fine imposed by any privacy regulator globally by many multiples.

The settlement also contains a number of novel and notable injunctive relief provisions, including mandated corporate governance changes at the company. The proposed settlement requires the creation of two new committees of the Board of Directors: one to oversee the company's privacy program, and one composed of independent directors to nominate the privacy committee members. In addition, the order requires that a designated compliance officer and the CEO Mark Zuckerberg make quarterly and annual compliance certifications on behalf of the company.

These new provisions go significantly beyond the kind of remedies the Bureau of Consumer Protection has sought in the past. They may reflect a new norm in the Commission's approach to privacy remedies, and the types of steps it could assert are required of e-commerce and technology companies possessing substantial consumer data. The settlement demonstrates the ways in which the FTC is thinking creatively about new tools to ensure appropriate privacy practices and its view of adequate disclosure to users as the internet and e-commerce present new risks for consumers.

Conclusion

The Commission's steady-growth approach to enforcing the consumer protection laws in e-commerce may be less likely to generate headlines than launching a new Technology Division, but it is no less significant. Collectively, the enforcement programs outlined above—which by no means include the entirety of the Bureau of Consumer Protection activity implicating technology and e-commerce—reflect scores of enforcement actions, billions of dollars in monetary remedies, and impact every aspect of consumers' online experience. ■

---

[1] Press Release, U.S. Dep't of Justice, Justice Department Reviewing the Practices of Market-Leading Online Platforms (July 23, 2019), https://www.justice.gov/opa/pr/justice-department-reviewing-practices-market-leading-online-platforms.

[2] Press Release, Fed. Trade Comm'n, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

[3] Dissenting Statement of Commissioner Rebecca Kelly Slaughter, In the Matter of Google LLC and YouTube, LLC (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542971/slaughter_google_youtube_statement.pdf (dissenting from the FTC settlement in the YouTube matter described below and stating that "The settlement is

impressive as far as it goes, but, for reasons I explain in more detail below, I am concerned that it does not go far enough"); Dissenting Statement of Commissioner Rohit Chopra, In the Matter of Google LLC and YouTube, LLC, FTC File No. 1723083 (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf (characterizing the injunctive provisions and monetary penalty amount in the YouTube settlement as insufficient and urging Congress to pass privacy legislation that would give "*all* enforcers of any privacy law a robust set of enforcement tools").

[4] Fed. Trade Comm'n, .com Disclosures, How to Make Effective Disclosures in Digital Advertising (Mar. 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.

[5] FTC v. DirecTV, Inc., No. 15-cv-01129-HSG, 2018 WL 3911196, at *1 (N.D. Cal. Aug. 16, 2018).

[6] Lesley Fair, Fed. Trade Comm'n, *FTC Says DIRECTV Wasn't So Direct About Fees and Negative Options*, Fed. Trade Comm'n Consumer Info. Blog (Mar. 11, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/ftc-says-directv-wasnt-so-direct-about-fees-negative-options.

[7] *Id.*

[8] FTC v. DirecTV, Inc., No. 15-cv-01129-HSG, 2018 WL 3911196, at *21 (N.D. Cal. Aug. 16, 2018).

[9] *Id.* at *19.

[10] *See, e.g.*, Stipulation of Voluntary Dismissal, FTC v. DirecTV, Inc., No. 15-cv-01129-HSG (Oct. 22, 2018) (providing no substantive explanation for dismissal); Dorothy Atkins, *FTC Drops $4B False Ad Suit Against DirecTV Midtrial*, Law360 (Oct. 22, 2018) (noting that the FTC declined to comment on its dismissal of the action against DirecTV).

[11] FTC v. Cyberspace.com LLC, 453 F.3d 1196, 1198–99 (9th Cir. 2006).

[12] FTC v. Grant Connect, LLC, 827 F. Supp. 2d 1199 (D. Nev. 2011).

[13] FTC Workshop, *Putting Disclosures to the Test* (Sept. 15, 2016), https://www.ftc.gov/news-events/events-calendar/2016/09/putting-disclosures-test.

[14] *Putting Disclosures to the Test*, Fed. Trade Comm'n (Nov. 2016), https://www.ftc.gov/system/files/documents/public_events/950633/disclosures-workshop-staff-summary-update.pdf.

[15] FTC Workshop, *An FTC Workshop About Online Ticket Sales* (June 11, 2019), https://www.ftc.gov/news-events/events-calendar/2019/03/online-event-tickets-workshop.

[16] Press Release, Fed Trade Comm'n, FTC Warns Hotel Operators that Price Quotes that Exclude 'Resort Fees' and Other Mandatory Surcharges May be Deceptive (Nov. 28, 2012), https://www.ftc.gov/news-events/press-releases/2012/11/ftc-warns-hotel-operators-price-quotes-exclude-resort-fees-other.

[17] FTC Workshop, *An FTC Workshop About Online Ticket Sales* (June 12, 2019), https://www.ftc.gov/news-events/audio-video/video/online-event-tickets-workshop-ftc-workshop-about-online-ticket-sales.

[18] *See, e.g.*, Call for Papers, 2nd Marketing Science-FTC Conferences on Marketing and Consumer Protection (Oct. 2, 2020), https://www.ftc.gov/system/files/documents/public_events/1567631/mrktscience-call-4-papers-2020_0.pdf.

[19] Tony Chen et al., *Thinking Inside the Subscription Box: New Research on e-commerce Consumers*, McKinsey & Company (Feb. 2018), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/thinking-inside-the-subscription-box-new-research-on-ecommerce-consumers.

[20] *See, e.g.*, Fed. Trade Comm'n, *Negative Options: A Report by the Staff of the FTC's Division of Enforcement* (Jan. 2009), https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf.

[21] Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401–8405.

[22] Press Release, Fed. Trade Comm'n, Online Lingerie Marketer Prohibited from Deceiving Shoppers About Negative-Option Programs (Nov. 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/11/online-lingerie-marketer-prohibited-deceiving-shoppers-about.

[23] FTC v. AdoreMe, Inc., No. 1:17-cv-09083 (S.D.N.Y. Nov. 21, 2017).

[24] FTC v. AH Media Group, LLC, No. 3:19-cv-4022 (N.D. Cal. Sept. 12, 2019).

[25] *See, e.g.*, FTC v. Triangle Media Corp., No. 18-cv-1388 (S.D. Cal. June 25, 2018); Lisa Lake, *Free Trials and Tribulations*, Fed. Trade Comm'n Consumer Info. Blog (Sept. 6, 2019), https://www.consumer.ftc.gov/blog/2019/09/free-trials-and-tribulations.

[26] 16 C.F.R. § 425.1.

[27] Press Release, Fed. Trade Comm'n, FTC Seeks Public Comment on Ways to Improve Current Requirements for Negative Option Marketing (Sept. 25, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/ftc-seeks-public-comment-ways-improve-current-requirements.

[28] Plaintiff's Response in Opposition to Defendant's Motion to Dismiss at 5, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[29] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015).

[30] LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

[31] Complaint ¶ 10, LabMd, Inc., FTC Docket No. 9357 (Aug. 29, 2013).

[32] Administrative Law Judge Initial Decision at 88, LabMd, Inc., FTC Docket No. 9357 (Nov. 13, 2015).

[33] Commission Opinion at 1, LabMD, Inc., FTC Docket No. 9357 (July 29, 2016).

[34] *LabMD*, 894 F.3d at 1236.

[35] Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, Fed Trade Comm'n Bus. Blog (Jan. 6, 2020, 9:46 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

[36] FTC v. Equifax Inc., No. 1:19-cv-03297-TWT (N.D. Ga. July 23, 2019).

[37] *See, e.g.*, GMR Transcription Servs., Inc., FTC No. C-3382 (Aug. 14, 2014) (alleging medical transcription company unfairly exposed consumers' medical information, in part because it failed to require independent contractors to implement reasonable security measures).

[38] *See, e.g.*, FTC v. D-Link Corp., No. 3:17-cv-00039 (N.D. Cal. Jan. 5, 2017) (alleging company misrepresented security of internet-connected devices and exposed consumer data to hackers).

[39] FTC v. Educare Ctr. Serv., Inc., No. 3:19-cv-00196-KC (W.D. Tex. Dec. 3, 2019).

[40] Press Release, Fed. Trade Comm'n, FTC Warns 19 VoIP Service Providers That 'Assisting and Facilitating' Illegal Telemarketing or Robocalling Is Against the Law (Jan. 30, 2020), https://www.ftc.gov/news-events/press-releases/2020/01/ftc-warns-19-voip-service-providers-assisting-facilitating.

[41] Press Release, Fed. Trade Comm'n, FTC and FCC Send Joint Letters to VoIP Service Providers Warning Against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls (Apr. 3, 2020), https://www.ftc.gov/news-events/press-releases/2020/04/ftc-fcc-send-joint-letters-voip-service-providers-warning-against.

[42] FTC v. Match Group, Inc., No. 3:19-02281 (N.D. Tex. Sept. 25, 2019). Match Group, Inc. is contesting all of the allegations in the litigation.

[43] 16 C.F.R. § 312.

[44] The settlement with YouTube involved both the FTC and the New York State Attorney General. Under the settlement, YouTube paid $136 million of the civil penalty to the FTC and $34 million to the State of New York.

[45] Lesley Fair, *Largest FTC COPPA Settlement Requires Musical.ly to Change Its Tune*, Fed. Trade Comm'n Bus. Blog (Feb. 27, 2019, 12:57 PM), https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its.

[46] *Upcoming Changes to Kids Content on YouTube.com*, YouTube Help, https://support.google.com/youtube/answer/9383587?hl=en.

[47] Statement of Chairman Joseph Simons and Commissioner Christine Wilson, In the Matter of Google LLC and YouTube, LLC (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf.

[48] Statement of Commissioner Rohit Chopra, In the Matter of Google LLC and

YouTube, LLC (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

[49] *See, e.g.*, T&M Protection Resources, LLC, FTC No. C-4709 (Mar. 16, 2020); Unrollme Inc., FTC No. C-4692 (Dec. 16, 2019); RagingWire Data Centers, Inc., FTC No. C-9386 (Nov. 5, 2019); ReadyTech Corp., FTC No. C-4659 (Oct. 17, 2018); VenPath Inc., FTC No. C-4664 (Nov. 15, 2018); United States v. Sunkey Publ'g, No. 3:18-cv-01444-HNJ (N.D. Ala. Sept. 6, 2018); FTC File No. 162-3211 (2018); BLU Products and Samuel Ohev-Zion, FTC No. C-4657 (Sept. 6, 2018); PayPal, Inc., FTC No. C-4651 (May 23, 2018).

[50] *See, e.g.*, Prepared Remarks of Chairman Joseph J. Simons at the May 8, 2019 Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security" at the Committee on Energy and Commerce, subcommittee on Consumer Protection and Commerce, https://www.ftc.gov/system/files/documents/public_statements/1519226/2019_ec_oral_remarks.pdf.

[51] Federal Trade Commission Staff Comment on the Preliminary Draft for the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (Oct. 24, 2019), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-preliminary-draft-nist-privacy-framework/p205400nistprivacyframeworkcomment.pdf.

[52] Press Release, Fed. Trade Comm'n, 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.