TECH SERVICES ARE EXTENSIVELY REGULATED

Introduction

Tech services are highly regulated in the United States in their offerings to consumers, how they interact with their workforces, and in their competition with the numerous companies that compete for consumers' attention. Multiple frameworks have been developed by federal and state agencies and legislatures, as well as self-regulatory organizations. Federal and state enforcers, self-regulatory watchdogs, and private litigants enforce the numerous laws and rules aggressively. Perhaps most importantly, federal and state regulators have brought countless enforcement actions against tech companies to enforce privacy, consumer protection, and competition laws. For example, the Federal Trade Commission ("FTC") alone has brought consumer protection and competition actions against dozens of major tech companies, including Facebook, Apple, Google, Microsoft, Twitter, Amazon, Oracle, and many others. In the privacy space, the FTC has brought over 75 general privacy cases and 65 data security cases since 2002.

In the privacy space, the FTC has brought over 75 general privacy cases and 65 data security cases since 2002.

These robust requirements, coupled with aggressive enforcement, are part of a balanced regulatory approach that allows the Internet to grow and power the economy. Any new enforcement approach must be similarly balanced--it should solve a proven and specific harm to consumers and avoid causing unnecessary damage to the economy.

Indeed, the federal government has a multifaceted approach to overseeing the technology industry. Contrary to the image of stagnant government enforcement, for example, the FTC recently debuted its new Technology Task Force within the Bureau of Competition.[1]

- The FTC's Office of Technology Research and Investigation employs technologists to support tech-focused investigations and produce original technical research, and its Tech Lab provides undercover Internet access and innovative tools to support technical investigations and capture evidence.[2]
- The Department of Justice ("DOJ") Antitrust Division likewise has an investigation and litigation section dedicated to the field: the Technology and Financial Services Section, consisting of

[1] FTC, "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.

[2] FTC, "How the FTC keeps up on technology," (Jan. 4, 2018), https://www.ftc.gov/news-events/blogs/techftc/ 2018/01/how-ftc-keeps-technology.

approximately 30 lawyers.[3] It also has a Telecommunications and Broadband Section, again consisting of approximately 30 lawyers.[4]

Several other agencies have technology-dedicated teams, such as the:

- Cybersecurity Program and Computer Crimes Unit at the Department of Health and Human Services ("HHS"),[5]
- Cybersecurity Unit at the Securities and Exchange Commission ("SEC"),[6] and
- Consumer Policy Division & Information Access & Privacy Office at the Federal Communications Commission ("FCC").[7]

The federal agencies also cooperate with each other on technology issues, both on enforcement and policy. Frequent collaborators include the FTC, DOJ, FCC, Food and Drug Administration, Department of Transportation, Department of Commerce, Department of Defense, Patent and Trademark Office,

Government Agencies With Oversight Over Tech Businesses

[3] *See* Section web page at https://www.justice.gov/atr/about-division/tfs-section.

[4] *See* Section web page at https://www.justice.gov/atr/about-division/telecommunications-and-broadband-section.

[5] HHS Cybersecurity Program, https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/information-security-privacy-program/index.html; HHS Computer Crimes Unit, https://oig.hhs.gov/reports-and-publications/featured-topics/cybersecurity/.

[6] SEC Press Release, "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors," Sept. 25, 2017, https://www.sec.gov/news/press-release/2017-176.

[7] FCC Consumer Policy Division & Information Access & Privacy Office, https://www.fcc.gov/general/consumer-and-governmental-affairs-bureau.

Federal Energy Regulatory Commission, HHS, and others. This creates a constellation of government agencies, each with unique and specialized technology experience and substantive knowledge, which amplifies the agencies' knowledge of industry trends.

As a matter of substance, three robust legal regimes regulate how tech companies (i) interact with consumers, (ii) manage content, and (iii) compete and otherwise interact with businesses. This comment provides a high level overview of each of these legal regimes, and follows with a detailed outline of the laws, regulations, guidelines, cases, and other materials that support the overview.

Existing Privacy Laws Regulating Tech Businesses

- Cable Communications Policy Act
- Cable Communications Policy Act
- Family Educational Rights and Privacy Act
- Computer Fraud and Abuse Act
- Drivers Privacy Protection Act
- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act
- Health Insurance Portability and Accountability Act
- Pen Register Act
- Foreign Intelligence Surveillance Act
- Privacy Act
- Privacy Protection Act
- Right to Financial Privacy Act
- Stored Communications Act
- Telephone Consumer Protection Act
- Video Privacy Protection Act
- CAN-SPAM Act
- Right to Financial Privacy Act
- Stored Communications Act
- Wiretap Act
- Children's Online Privacy Protection Act
- California Consumer Privacy Act of 2018
- State Unfair and Deceptive Acts and Practices Acts
- State Radio Frequency Identification Acts
- State Eraser Button Laws
- State Biometric Privacy Acts
- California Online Privacy Protection Act
- Vermont's Data Broker Regulation
- State Spyware laws
- California's Shine the Light Law
- 50 State Data Breach Laws
- State Student Privacy Laws
- Americans with Disabilities Act

Consumer Protection

Strict rules with robust enforcement govern consumers' relationship with tech services. Federal and state laws and regulations significantly constrain tech companies' digital practices, and govern numerous aspects of tech companies' businesses. The FTC is the top consumer protection enforcer in the U.S., including in the areas of privacy and data security, and has obtained consumer protection orders against many tech companies including Facebook, Microsoft, Google, Apple, Amazon, Oracle, Uber, PayPal, Snap, Vizio, HTC, Twitter, Yelp, Myspace, Lenovo, Sony BMG, and others. It

aggressively enforces Section 5 of the FTC Act, which prohibits unfair and deceptive practices, and interprets Section 5 broadly such that it covers a wide variety of consumer protection topics. ***See sections 1.A.i-iv below for more detail.***

Specifically on privacy, the FTC uses its Section 5 authority to bring enforcement actions against tech companies for allegedly engaging in unfair and deceptive practices. These actions have targeted a wide range of issues and categories of data, including, for example: location data, cookies and targeted advertising, privacy controls, retail analytics, TV viewing data, and more. With its strong enforcement culture, the FTC imposes orders on tech companies that contain significant privacy obligations with 20-year terms, including the implementation of comprehensive privacy programs, biennial assessments by independent experts, deletion of information alleged to have been illegally obtained, and robust transparency and choice mechanisms for consumers. ***See section 1.A.i below for more detail.***

The Commission can also obtain civil penalties for violations of its consent orders. For example, the FTC levied a $22.5 million penalty against Google for allegedly violating a consent order in 2012, and is expected to obtain a historic civil penalty ranging in the billions of dollars from Facebook in connection with its ongoing investigation of the company for alleged violations of its 2011 consent order. ***See section 1.A.i below for more detail.***

The FTC also brings actions against companies, including a number of tech companies like Facebook and Google, for falsely claiming participation in the EU-U.S. and Swiss-U.S. Privacy Shield Framework and its predecessor, the Safe Harbor Framework, or failing to comply with its principles. ***See section 1.A.i below for more detail.***

In addition to Section 5, the FTC enforces sector-specific laws that govern sensitive data such as children's data, financial data, and health data. For example, the Commission enforces the Children's Online Privacy Protection Act (COPPA) Rule, which requires companies to obtain verifiable parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought at least 25 cases under the COPPA Rule, including against tech companies, and has obtained at least $12.7 million in civil penalties for alleged violations of the Rule.[8] ***See section 1.A.ii below for more detail.***

The FTC also uses its Section 5 authority to bring cases against companies that fail to implement reasonable data security measures and/or suffer data breaches that expose consumers to unreasonable risk of harm. For example, in 2010, the FTC brought a Section 5 case against Twitter for allegedly deceiving consumers and putting their privacy at risk by failing to safeguard their personal information. Among other things, the FTC alleged that Twitter's missteps allowed hackers to obtain unauthorized control over the social media platform, including access to non-public user information and private tweets.[9] Pursuant to its Section 5 authority, the FTC has brought: deception actions against tech companies for making inaccurate representations about their data security measures; unfairness actions against tech companies for failing to employ reasonable and appropriate security measures to protect personal information; and actions against tech companies for failing to meet the security standards set forth in the COPPA Rule and the GLBA Safeguards Rule, among others. Actions have been brought where the FTC has alleged inadequate security, even where no breach has occurred.[10] An FTC data security investigation typically results in a settlement involving a 20-year consent order requiring, among other things, that the company implement a comprehensive data security program and obtain biennial assessments of that program from an independent third party. ***See section 1.A.iii below for more detail.***

An FTC data security investigation typically results in a settlement involving a 20-year consent order requiring, among other things, that the company implement a comprehensive data security program and obtain biennial assessments of that program from an independent third party.

The FTC is not the only privacy enforcer at the federal level. Federal agencies issue and enforce regulations of digital practices based on sector-specific laws, often in addition to the FTC, particularly in areas that impact sensitive data. For example, HHS enforces Privacy, Security, and Breach Notification Rules that govern the access, use, and maintenance of personal health information, and impose notification requirements on companies that experience a breach of personal health information. The SEC has also released formal cybersecurity guidance that requires companies to disclose material cybersecurity risks and costs, including in annual reports, and highlights other issues raised by

[8] GAO Report on Internet Privacy, January 2019, *available at* https://www.gao.gov/assets/700/696437.pdf.

[9] *In the Matter of Twitter, Inc.*, Dkt. No. C-4316 (June 24, 2010).

[10] *In the Matter of HTC America, Inc.*, Dkt. No. C-4406 (F.T.C. Feb. 22, 2013).

cybersecurity incidents (e.g., ensuring directors and officers do not engage in trading before incidents are made public).[11] Shortly after releasing this guidance, the SEC announced a $35 million settlement with Altaba, Inc. (f/d/b/a Yahoo! Inc.) for failing to adequately investigate and disclose a data breach that compromised hundreds of millions of user accounts.[12] ***See section 1.A.ii below for more detail.***

In addition to privacy and data security enforcement, the FTC uses its Section 5 authority to bring actions against tech companies for engaging in unfair and deceptive practices unrelated to privacy and data security. For example, the FTC has brought cases against tech companies for allegedly making false claims about their products, misrepresenting the features of their products, selling falsely or deceptively labeled products, and unfairly billing consumers for certain products or services. Companies including Apple, Amazon, Google, Facebook, Dish TV, and others have been subject to such FTC actions. The Commission uses its Section 5 authority to bring enforcement actions against large tech companies that fail to make clear and conspicuous disclosures online. It also brings actions against companies that install adware and other software on consumers' computers without their knowledge or consent, and against social media influencers that fail to disclose material connections with advertisers. ***See section 1.A.iv below for more detail.***

Categories of enforcement areas:

- Federal, state and local laws and regulations
- Governmental enforcement
- Private litigants

Federal agency regulation of tech companies' interactions with consumers is supplemented by rigorous regulation and enforcement on the state level. State enforcers do far more than merely duplicate or join enforcement actions taken by federal authorities; state laws are often substantively different from and augment federal laws. They impose a mosaic of obligations on tech companies, such as mandatory disclosures that provide consumers with the right to know how their data is being shared, and notice and consent requirements to collect biometric data. All 50 states have enacted data breach notification laws that impose increasingly onerous requirements on tech companies, and some states have enacted their own data security laws and regulations that apply to specific types of data (e.g., student data). In addition, state attorneys general use their authority under "little FTC Acts" and related consumer protection laws, including privacy and data security laws, consumer fraud laws, and select federal laws, to bring enforcement actions against tech companies. States have significant remedial power under these laws, and can obtain civil penalties of up to $50,000 per violation for violations of "little FTC Acts."[13]

[11] SEC Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 26, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[12] In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc., No. 3-18448 (April 24, 2018).

[13] *See, e.g.*, D.C. Code Ann. § 28-3905(i) ($1,000); 815 I. ILCS 505/7(b) ($50,000).

States have significant remedial power under these laws, and can obtain civil penalties of up to $50,000 per violation for violations of "little FTC Acts."

States have used this authority to investigate companies for data breaches, violations of state eavesdropping laws, state customer records laws, and the COPPA Rule, among other things. For example, the DC attorney general recently sued Facebook under the DC Consumer Protection Procedures Act for, among other things, misleading consumers about the security of their data and failing to properly monitor third party apps' use of data.[14] In 2013, Google paid $17 million to settle multistate allegations that the company circumvented users' browser privacy settings.[15] State attorneys general are also active COPPA enforcers, having brought at least 15 COPPA cases since 2007. Many of these cases result in substantial penalties; for example, the New York attorney general recently settled a COPPA case against Oath (f/k/a AOL) for $4.5 million.[16] ***See section 1.B below for more detail.***

In addition, robust self-regulatory regimes provide additional protections for consumers, particularly in the advertising arena.[17] The FTC has been a long-standing and vocal supporter of self-regulatory programs, and has warned businesses that "[m]embership in self-regulatory programs is your call, but once you advertise your adherence to an industry code, live up to its terms."[18] Many of these programs require public tech companies that submit to the programs to make commitments to the self-regulatory codes that, if violated, can result in government investigation and enforcement. The FTC also reviews compliance with relevant self-regulatory codes in the course of its investigations.[19] ***See section 1.D below for more detail.***

Finally, private litigants bring actions against tech companies under federal and state privacy and data security laws and other novel theories of liability. For example, private plaintiffs have brought actions against tech platforms for allegedly collecting and using information in violation of federal and state wiretapping laws, federal computer crime laws, and state consumer fraud laws, among others. Between

---

[14] DCAG Press Release, AG Racine Sues Facebook for Failing to Protect Millions of Users' Data (Dec. 19, 2019), *available at* https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions.

[15] *In the Matter of Google Inc.*, No. ____ (Nov. 18, 2013), *available at* https://portal.ct.gov/-/media/AG/Press_Releases/2013/20131118GoogleSafariAVCExecutedpdf.pdf?la=en.

[16] NYAG Press Release, A.G. Underwood Announces Record COPPA Settlement with Oath - Formerly AOL - For Violating Children's Privacy (Dec. 4, 2018), *available at* https://ag.ny.gov/press-release/ag-underwood-announces-record-coppa-settlement-oath-formerly-aol-violating-childrens.

[17] *E.g.*, Network Advertising Initiative, https://www.networkadvertising.org/; Digital Advertising Alliance, https://digitaladvertisingalliance.org/; Student Privacy Pledge, https://studentprivacypledge.org/.

[18] FTC Business Blog, Track afield: What the FTC's Google case means for your company (Aug. 13, 2012), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2012/08/track-afield-what-ftcs-google-case-means-your-company.

[19] *See* FTC Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

2013 and 2014, plaintiffs filed approximately 672 complaints alleging privacy violations in U.S. district courts.20 Both the high costs and severe consequences associated with private litigation, and the increasing frequency of that litigation, creates incentives for technology companies to comply with regulations, take proactive steps to protect consumers, and ensure they are following industry best practices. These actions are typically filed on behalf of a class, and thus involve substantial discovery and motion practice costs associated with class certification. Many also result in significant monetary settlements and public injunctive relief. For example, in 2012, Netflix paid $9 million to settle a class action alleging violations of the Video Privacy Protection Act.21 In 2018, tech companies including Twitter, Instagram, Yelp, and Foursquare agreed to pay $5.3 million to settle class allegations that the companies uploaded users' address book data without their knowledge or consent.22 More recently, Vizio agreed to pay $17 million to settle multidistrict allegations that the company collected and sold consumers' data for advertising purposes without their knowledge or consent.23 Technology services companies will remain primary targets of an active plaintiffs' bar given the success of the technology sector and opportunities for significant recoveries and settlements. See section 1.C below for more detail.

Platform Responsibility

Technology platforms face civil and criminal liability for content on their platforms under a host of laws, including federal copyright and obscenity laws. Section 230 of the Communications Decency Act ("CDA 230") gives platforms immunity from content liability in certain circumstances, but does not shield them from all forms of liability, including criminal liability, and incentivizes platforms to police user generated content. For example, because the CDA states that IP laws remain in full force,[24] tech companies can face liability for third-party copyright infringement unless their actions fall under the safe harbors under the Digital Millennium Copyright Act ("DMCA").[25] Tech platforms also have incentives to vigorously regulate content on their platforms because CDA 230 makes clear that service providers cannot be held liable for engaging in good faith action to exclude or limit access to objectionable content.[26] For example, leading technology platforms like YouTube, Facebook, and Twitter maintain community guidelines and similar policies and procedures that govern the treatment of nudity

---

[20] *Engineered Liability: The Plaintiffs' Bar's Campaign to Expand Data Privacy and Security Litigation*, U.S. Chamber Institute for Legal Reform, April 2017, *available at* https://www.instituteforlegalreform.com/research/engineered-liability-the-plantiffs-bars-campaign-to-expand-data-prviacy-and-security-litigation.

[21] *In re: Netflix Privacy Litig.*, No. 5:11-cv-00379 (Sept. 5, 2012).

[22] Marc Opperman, et al. v. Kong Tech., Inc., et al., No. 13-cv-00453 (N.D. Cal. Mar. 27, 2018).

[23] In re: Vizio, Inc., Consumer Privacy Litigation, No. 8:16-ml-02693 (C.D. Cal. Jan. 4, 2019).

[24] 47 U.S.C. § 230(e)(2).

[25] 17 U.S.C. § 512 *et seq.*

[26] *See Batzel v. Smith*, 333 F.3d 1018, 1028 (9th Cir. 2003) (Congress intended "to encourage interactive computer services and users of such services to self-police").

and sexual content, hateful content, violent content, cyberbullying, spam, threats, and similar content.[27] They also provide users with safety settings and other tools to report objectionable content.[28] ***See section 2.A below for more detail.***

Tech platforms also have incentives to vigorously regulate content on their platforms because CDA 230 makes clear that service providers cannot be held liable for engaging in good faith action to exclude or limit access to objectionable content.

Tech platforms also face liability under discrimination laws when they "develop" content on their platforms. Section 230 of the CDA only protects tech platforms in their capacity as platforms on which others post content. To the extent that the platform itself has a direct hand in creating the allegedly offending content, it may be held liable. For example, a digital platform that helped apartment renters find suitable roommates was found liable for violating fair housing laws when it created forms requiring users to upload information about sex, family status, and sexual orientation and preferences regarding those traits in potential roommates.[29] The platform's active role in creating and developing content that was used to violate housing discrimination laws disqualified it from CDA protection. ***See section 2.B below for more detail.***

Tech platforms also face liability for election advertisements disseminated on their platforms. The Federal Election Commission ("FEC") has long regulated political ad disclosures, and is currently seeking to expand its authority to regulate platforms that host political content. In addition, states have passed a number of laws requiring platforms to maintain and publish records relating to political ads and verify advertiser registration with state officials, among other things. State officials have used these laws to bring actions against large tech companies like Facebook and Google. ***See section 2.C below for more detail.***

Business Conduct

In addition to special-purpose regulation, tech businesses are also extensively regulated by the same agencies and laws that regulate other corporations. This includes the antitrust laws - which are enforced by both state and federal regulators, including both the FTC and DOJ - but also includes

[27] See, e.g., YouTube Community Guidelines, https://www.youtube.com/yt/about/policies/#community-guidelines; Twitter Hateful Conduct Policy, https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy; Facebook Community Standards, https://www.facebook.com/communitystandards/.

[28] See, e.g., YouTube Community Guidelines Reporting and Enforcement, https://www.youtube.com/yt/about/policies/#reporting-and-enforcement; Twitter Report a Tweet or Direct Message, https://help.twitter.com/en/safety-and-security/report-a-tweet.

[29] Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).

labor law, financial services law, tort law, and much more. These regulatory regimes interlock to require tech companies to act responsibly, and to protect the interests of consumers and the public at large.

Traditional antitrust and business law -- enforced by federal and state regulators, as well as private plaintiffs -- provides robust checks on all business conduct, including that of technology services providers. Antitrust law in particular has frequently been used to prevent conduct by tech companies that would reduce the welfare of consumers (e.g., "the consumer welfare standard") - whether by increasing prices, or by reducing the quality, availability, or rate of innovation in technological goods and services.

The DOJ and the FTC also cooperate with other federal agencies involving technology issues relevant to antitrust issues. Many of these agencies also have competition authority and apply competition principles when conducting their own regulatory reviews; for example, DOJ is a member of the intra-governmental Committee on Foreign Investment in the United States (CFIUS), which reviews national security-sensitive transactions, including mergers and acquisitions, many of which involve transactions in high tech industries. CFIUS has blocked or caused the withdrawal of many technology transactions involving foreign buyers, including Broadcom's attempted acquisition of Qualcomm in 2018. Robust laws and regulators constrain how tech services conduct themselves in the market.

In addition to the overarching requirements of the consumer welfare standard, the DOJ and the FTC maintain multiple policy statements and official guidelines that apply to the technology industry, including the Antitrust Policy Statement on Sharing of Cybersecurity Information[30] and the Antitrust Guidelines for the Licensing of Intellectual Property.[31] The recent crackdown on technology companies' "no poach" policies have ensnared virtually every major technology company.[32] The DOJ criminally prosecuted an online purveyor of posters for using algorithms to fix prices with competitors.[33] Separately, the possibility of contingency fees based on treble damages awards is a powerful incentive to ensure that plaintiffs' attorneys leave few meritorious cases unfiled. These are all part of a long pattern of aggressive antitrust enforcement in the technology space, going back to government's long-standing competition enforcement efforts against companies such as AT&T, IBM, Microsoft, Google, Intel, and other technology firms. Indeed, DOJ and the FTC themselves have brought many antitrust enforcement actions involving technology industries. This has been true historically with landmark cases against AT&T and Bell Labs, IBM, Microsoft, and Intel, and more recent examples set forth below.

---

[30] DOJ and FTC Antitrust Policy Statement on Sharing of Cybersecurity Information (April 2014), *available at* https://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf.

[31] DOJ and FTC Antitrust Guidelines for the Licensing of Intellectual Property (Jan. 2017), *available at* https://www.justice.gov/atr/IPguidelines/download.

[32] *E.g.*, *United States v. eBay, Inc.*, No. 12-cv-5869, Final Judgment, Doc. 66 (N.D. Cal. Sept. 2, 2014); *United States v. Adobe Sys., Inc.*, No. 1:10-cv-1629, Final Judgment, Doc. 17 (D.D.C. Mar. 18, 2011); *see United States v. Lucasfilm Ltd.*, No. 1:10-cv-2220, Final Judgment, Doc. 6-1 (D.D.C. May 9, 2011); Press Release, Dep't of Justice, Justice Department Requires Six High Tech Companies to Stop Entering into Anticompetitive Employee Solicitation Agreements (Sept. 24, 2010), *available at* https://www.justice.gov/opa/pr/justice-department-requires-six-high-tech- companies-stop-enteringanticompetitive-employee.

[33] *See United States v. Tompkins*, No. 15-cr-201 (N.D. Cal., filed Apr. 6, 2015).

Antitrust lawyers typically divide enforcement into four categories -- cartels, mergers, joint conduct, and single firm conduct -- so this paper organizes enforcement action citations accordingly. ***See section 3.A.i-ii below for more detail.***

Antitrust law has also served as a basis for regulating mergers in the technology space.

Antitrust law has also served as a basis for regulating mergers in the technology space. Among many notable precedents, the DOJ blocked Google's proposed 2008 partnership with Yahoo!, arguing that it would harm competition in Internet search advertising and syndication.[34] DOJ also successfully unwound a consummated merger between PowerReviews and Bazaarvoice, the two top providers of third-party ratings and reviews functionality,[35] and extracted data-sharing requirements from Google in its acquisition of travel information provider ITA.[36] ***See section 3.A.iii below for more detail.***

Many of the attempts to regulate the technology industry via antitrust litigation break new ground and apply traditional antitrust principles to new technology. Perhaps the best-known example is the years of antitrust litigation between DOJ and Microsoft, starting in the 1990s.[37] More recently, the FTC successfully litigated against 1-800 Contacts, alleging that a series of IP infringement settlements reduced competition for online advertising.[38] In the wake of that case, other somewhat similar private cases have been filed against competing companies that colluded by agreeing to refrain from purchasing each others' brand names as key terms used for online advertising.[39] The government has targeted technology companies in particular through litigation aimed at violations of standard essential patent holders' FRAND commitments and licensing practices.[40] ***See section 3.A .iv below for more detail.***

Other areas of corporate regulation, such as labor and discrimination laws, product liability laws, securities and financial regulation, and many more, are also used in innovative ways to regulate technology firms' business models and labor practices. For example, technology platforms that are predicated upon independent contractors who work when and where they please face numerous

[34] *See* DOJ Press Release, Yahoo! Inc. and Google Inc. Abandon Their Advertising Agreement (Nov. 5, 2008), *available at* https://www.justice.gov/archive/opa/pr/2008/November/08-at-981.html.

[35] *See U.S. v. Bazaarvoice, Inc.*, No. 13-0133 (N.D. Cal. 2013).

[36] See U.S. v. Google Inc. and ITA Software, Inc., 1:11-CV-00688 (D. D.C. April 2011).

[37] *United States v. Microsoft Corp.*, 56 F. 3d 1448 (D.C. Cir. 1995) (approving consent decree in the first DOJ antitrust litigation against Microsoft for bundling); see also *United States v. Microsoft Corp.*, No. 98-cv-01232 (D.D.C. May 18, 1998) (alleging a series of anticompetitive activities to protect Microsoft's monopoly in the market for PC operating systems); *United States v. Microsoft Corp.*, 253 F.3d 34 (D.C. Cir. 2001).

[38] *In re 1-800 Contacts, Inc.,* Dkt. No. 9372 (F.T.C. Aug. 8, 2016).

[39] *See Tichy v. Hyatt Hotels Corp. et al.*, No. 18-cv-1959 (N.D. Ill. filed Mar. 19, 2018).

[40] *E.g.*, *FTC v. Qualcomm Inc.*, No. 17-cv-00220 (N.D. Cal. Jan. 17, 2017).

lawsuits by workers challenging this model, many of which have settled for tens of millions of dollars.[41] In addition, although Uber and Lyft have claimed that they are technology providers, not transportation providers, and therefore immune from suits brought under the Americans with Disabilities Act ("ADA"), a federal court disagreed in December 2018.[42] This follows on the heels of a settlement of discrimination litigation brought against Uber by a class of blind passengers who alleged discriminatory treatment.[43]

The following provides a more detailed overview of all the ways in which technology services are regulated. We encourage the FTC to carefully consider the current enforcement framework as it evaluates its own enforcement and policy development over the coming years.

[41] *See, e.g.*, *Cotter v. Lyft, Inc.*, 13-cv-04065-VC (N.D.Ca.) (challenging independent contractor status and settling for $27 million).

[42] *See, e.g.*, *Access Living of Metro. Chi. v. Uber Techs.*, 351 F. Supp. 3d 1141 (N.D. Ill. 2018) (denying Uber's motion to dismiss that the ADA does not apply to it in lawsuit over wheelchair accessibility).

[43] *Nat'l Fed. of the Blind of Cal. v. Uber Techs.*, No. 14-cv-04086 ECF No. 84 (N.D. Cal. 2016) (approving settlement of class action alleging that Uber discriminated against blind passengers).

TECH SERVICES ARE EXTENSIVELY REGULATED

CONTENTS

NetChoice

1 - CONSUMER PROTECTION

A- Federal Privacy, Data Security, and Consumer Protection Regulations

i - General Privacy Enforcement

The FTC is the top privacy regulator in the U.S, where it has brought over 100 cases in the past decade.[44] In most of these matters, the FTC relies on its Section 5 authority (prohibiting unfair and deceptive acts or practices) to bring enforcement actions against tech companies alleging privacy violations. Examples include:

- *In the Matter of PayPal, Inc.*, Dkt. No. C-4651 (F.T.C. Feb. 27, 2018) (its peer-to-peer payment network Venmo, among other things, failed to disclose or adequately disclose consumers' ability to restrict the visibility of transactions);
- *In the Matter of Lenovo, Inc.*, Dkt. No. C-4636 (F.T.C. Sept. 15, 2017) (among other things, failed to disclose or adequately disclose that pre-installed software would collect consumers' sensitive communications and browsing data);

FTC is the top privacy regulator in the U.S, where it has brought over 100 cases in the past decade

- *In the Matter of Uber Technologies, Inc.*, Dkt. No. C-3054 (F.T.C. Aug. 15, 2017) (misrepresented the extent to which it monitored its employees' access to users' and drivers' personal information and the steps it took to secure that information);
- *FTC v. Vizio, Inc.*, No. 2:17-cv-00758 (D. N.J. Feb. 6, 2017) (installed software on its smart TVs to collect viewing data on 11 million consumer TVs without their knowledge or consent);
- *In the Matter of Turn, Inc.*, Dkt. No. C-4612 (F.T.C. Dec. 20, 2016) (tracked consumers online and through its mobile apps even after they took steps to opt-out of such tracking);
- *U.S. v. InMobi Pte Ltd.*, No. 3:16-cv-03474 (N.D. Cal. June 22, 2016) (among other things, represented that it tracked consumers' location and served geo-targeted ads only if the consumer had provided opt-in consent when in fact, it tracked consumers even if the consumer had not provided opt-in consent);
- *In the Matter of Practice Fusion, Inc.*, Dkt. No. C-4591 (F.T.C. June 8, 2016) (misled consumers by soliciting reviews for doctors in connection with an online healthcare survey without adequately disclosing that the reviews would be publicly posted online, resulting in the disclosure of patients' sensitive personal and medical information);
- *In the Matter of Nomi Technologies, Inc.*, Dkt. No. C-4538 (F.T.C. Sept. 3, 2015) (among other things, failed to provide an opt-out at retail locations as represented in its privacy policy);

[44] GAO Report on Internet Privacy, January 2019, *available at* https://www.gao.gov/assets/700/696437.pdf.

- *In the Matter of Snapchat, Inc.*, Dkt. No. C-4501 (F.T.C. May 8, 2014) (misrepresented extent to which it maintained the privacy, security, and confidentiality of users' information, including the disappearing nature of messages sent through the service);
- *In the Matter of Myspace, LLC*, Dkt. No. C-4369 (F.T.C. Sept. 11, 2012) (misrepresented that it would provide notice and obtain consent to use or share users' personal data except as described in the privacy policy);
- *In the Matter of Facebook, Inc.*, Dkt. No. C-4365 (F.T.C. Nov. 29, 2011) (told consumers they could keep their information private when in fact it was repeatedly shared and made public);
- *In the Matter of Google, Inc.*, Dkt. No. C-4336 (F.T.C. Oct. 24, 2011) (violation for using consumer information beyond the purpose for which it was collected when Google launched its social network, Google Buzz).

The FTC vigorously enforces these orders and obtains steep civil penalties for alleged violations. For example:

- The FTC has announced that it is investigating Facebook for alleged violations of a 2011 order prohibiting it from making deceptive privacy claims, among other things. According to news reports, the FTC plans to impose a historic civil penalty of around $5 billion on Facebook for these alleged violations;[45]
- *In the Matter of Uber Tech., Inc.*, No. C-4662 (F.T.C. Oct. 26, 2018) (expanded previous consent order, potentially exposing Uber to civil penalties if it fails to notify the FTC of certain future incidents involving unauthorized access to driver and rider information);
- *U.S. v. Upromise, Inc.*, No. 1:17-cv-10442 (D. Mass. Mar. 16, 2017) (obtained a $500,000 penalty for alleged violation of a 2012 consent order requiring Upromise to make disclosures about its data collection and use and to obtain third-party assessments of its data collection toolbar);
- *U.S. v. Google, Inc.*, No. 3:12-cv-04177 (N.D. Cal. Nov. 20, 2012) (obtained $22.5 million penalty for alleged violation of a 2011 order prohibiting Google from materially misrepresenting the extent to which customers could exercise control over the collection of their information).

FTC privacy settlements have been more than $30million.

The FTC also brings enforcement actions against companies for falsely claiming participation in the Privacy Shield and its predecessor, the Safe Harbor Framework, or failing to comply with their principles. To obtain Privacy Shield certification, companies are required to self-certify annually that they comply with a set of principles (e.g., notice and choice) for the transfer of data from the EU to the U.S. Thousands of companies are Privacy Shield certified, including large tech companies like Amazon,

[45] *See, e.g.*, E. Dwoskin and T. Romm, "Facebook sets aside billions of dollars for a potential FTC fine," Wash. Post, Apr. 24, 2019, https://www.washingtonpost.com/technology/2019/04/24/facebook-sets-aside-billions-dollars- potential-ftc-fine/.

Facebook, Google, Microsoft, Twitter, and Snap.[46] Examples of actions alleging tech companies made false claims about Privacy Shield and Safe Harbor participation or failed to comply with the framework principles include:

- *In the Matter of ReadyTech Corp.*, No. C-4659 (F.T.C. Oct. 17, 2018) (falsely claimed it was in the process of Privacy Shield certification);
- *In the Matter of True Comm., Inc., d/b/a TCPrinting.net*, No. C-4628 (F.T.C. Nov. 29, 2017) (falsely claimed participation in Privacy Shield);
- *In the Matter of Decusoft, LLC*, No. C-4630 (F.T.C. Nov. 20, 2017) (same);
- *In the Matter of Contract Logix, LLC*, No. C-4541 (F.T.C. Sept. 29, 2015) (falsely claimed compliance with Safe Harbor);
- *In the Matter of Apperian, Inc.*, No. C-4461 (F.T.C. June 19, 2014) (falsely claimed participation in Safe Harbor);
- *In the Matter of BitTorrent, Inc.*, No. C-4464 (F.T.C. June 19, 2014) (same);
- *In the Matter of DataMotion, Inc.*, No. C-4466 (F.T.C. June 19, 2014) (same);
- *In the Matter of Myspace, LLC*, No. C-4369 (F.T.C. Aug. 13, 2012) (failed to adhere to Safe Harbor notice and consent principles);
- *In the Matter of Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) (same);
- *In the Matter of Google, Inc.*, No. C-4336 (F.T.C. Oct. 13, 2011) (same).

ii - Sectoral Privacy Enforcement

Agencies issue and enforce regulations of digital practices based on sectoral laws, especially in areas impacting sensitive data (e.g., FTC rules on children's data; FTC, HHS, and FDA rules on health data; FTC and SEC rules on financial data). These agencies also issue specific guidance to companies based on their legal obligations, such as on data security, children's privacy, and more.

- Children's privacy: The FTC regulates tech companies' collection, use, and disclosure of children's personal information through its authority under the COPPA Rule.[47] Cases alleging violations of COPPA include, among others:
    - *U.S. v. Musical.ly*, No. 2:19-cv-01439 (C.D. Cal. Feb. 27, 2019) ($5.7 million fine for video social networking app's improper collection of personal information from children, the largest COPPA civil penalty in FTC history);
    - *U.S. v. VTech Electronics, Ltd.*, No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018) ($650,000 fine against electronic toy manufacturer for COPPA violations of improperly collecting personal information from children and failing to maintain reasonable security procedures to protect such information);

[46] Privacy Shield Participant List, https://www.privacyshield.gov/list.

[47] 16 C.F.R. Part 312.The COPPA Rule was adopted pursuant to the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505.

- *U.S. v. InMobi Pte Ltd.*, No. 3:16-cv-03474 (N.D. Cal. June 22, 2016) ($4 million penalty against the company for deceptively tracking children's location and serving them geo-targeted advertising without parental notice or consent);
- *U.S. v. Yelp, Inc.*, No. 3:14-cv-04163 (N.D. Cal. Sept. 17, 2014) ($450,000 penalty against Yelp for collecting children's names, email addresses, and location information without parental notice and consent).

- Health privacy:
  - Pursuant to its authority under HIPAA,[48] HHS has implemented and enforces Privacy, Security, and Breach Notification Rules that regulate companies' handling of personal health information (PHI).
    - These regulations apply to tech companies that use and disclose PHI or -- in their capacity as business associates to HIPAA covered entities -- otherwise create, receive, maintain, or transmit PHI on behalf of such companies.
    - The Privacy Rule restricts companies' access to, use, and disclosure of PHI; the Security Rule requires companies to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI; and the Breach Notification Rule imposes breach notification requirements on companies that suffer breaches of PHI.
    - Since 2003, HHS has obtained almost $100 million in civil penalties in cases alleging violations of HIPAA Rules.[49]
- Financial privacy:
  - The FTC has used its authority under the GLBA[50] to bring enforcement actions against tech companies for alleged violations of the GLBA's Safeguards Rule (which requires companies to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards), and the Privacy Rule (which requires companies to provide customers with clear and conspicuous initial and annual privacy notices detailing their privacy policies and practices).[51]

---

[48] Pub. L. 104-191.

[49] HHS Enforcement Highlights, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/ enforcement-highlights/index.html.

[50] 15 U.S.C. §§ 6801-6824.

[51] Safeguards Rule, 16 C.F.R. § 314; Privacy Rule, 16 C.F.R. § 313.

The FTC has used its authority under the GLBA[52] to bring enforcement actions against tech companies for alleged violations of the GLBA's Safeguards Rule

Cases alleging violations of financial privacy laws and regulations include:

- *In the Matter of PayPal, Inc.*, Dkt. No. C-4651 (F.T.C. Feb. 27, 2018) (violated the Safeguards and Privacy Rules by failing to assess reasonably foreseeable risks to customer information failing to provide privacy notices to customers);
- *In the Matter of TaxSlayer, LLC*, Dkt. No. C-4626 (F.T.C. Nov. 8, 2017) (online tax preparation service provider violated the Safeguards and Privacy Rules by failing to safeguard customer data and failing to provide privacy notices to customers);
- *ACRAnet Inc.*, Dkt. No. C-4330 (F.T.C. Aug. 19, 2011) (credit report resellers violated the Safeguards Rule by, among other things, failing to implement reasonable security safeguards and develop a comprehensive information security program, where consumer data was obtained via online hacking).

iii - Data Security

The FTC is also the leading federal agency that investigates data breaches, and has entered into more than 60 settlements with companies regarding their allegedly lax data security practices. Examples abound:

- *In the Matter of LightYear Dealer Techs., LLC d/b/a Dealerbuilt*, No. ____ (F.T.C. June 12, 2019) (software and data processing company failed to implement readily available and low-cost measures to protect auto dealer clients' personal data, for example, by storing and transmitting personal data in clear text without proper access and authentication controls);
- *In the Matter of PayPal, Inc.*, Dkt. No. C-4651 (F.T.C. Feb. 27, 2018) (peer-to-peer payment service Venmo failed to use bank-grade security systems and data encryption to protect customers' financial information as promised);
- *In the Matter of Lenovo, Inc.*, Dkt. No. C-4636 (F.T.C. Sept. 15, 2017) (pre-loaded software onto laptops that compromised security in order to deliver ads to consumers);
- *In the Matter of ASUSTeK Computer, Inc.*, File No. 142 3156 (F.T.C. Feb. 23, 2016) (failed to take reasonable steps to secure the software on its routers despite making promises about their security);
- *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530 (D. Ariz. Jan. 4, 2016) ($100 million civil penalty for violating the terms of a data security order requiring company to secure consumers' personal information and prohibiting deceptive advertising about its data security);
- *In the Matter of Oracle Corp.*, Dkt. No. C-4571 (F.T.C. Dec. 21, 2015) (deceived consumers about the level of security provided by its Java Platform Standard Edition software updates);

[52] 15 U.S.C. §§ 6801-6824.

- *In the Matter of Snapchat, Inc.*, Dkt. No. C-4501 (F.T.C. May 8, 2014) (deceived consumers regarding the security measures it took to protect data from misuse and unauthorized disclosure);
- *In the Matter of TRENDnet, Inc.*, Dkt. No. C-4426 (F.T.C. Sept. 4, 2013) (lax security practices by networking company led to exposure of private consumer video and audio feeds, despite marketing its products as "secure");
- *In the Matter of HTC America, Inc.*, Dkt. No. C-4406 (F.T.C. Feb. 22, 2013) (failed to take reasonable steps to secure software developed for its smartphones and tablets, introducing security flaws that placed sensitive information about millions of consumers at risk);
- *In the Matter of Twitter, Inc.*, No. C-4316 (F.T.C. June 24, 2010) (failed to safeguard users' personal information, allowing hackers to access non-public user information and tweets that consumers had designated as private).

The FTC recouped over $100million from data breach enforcements.

The SEC also has the authority to investigate data breaches under Regulation S-P's Safeguards Rule, which requires broker-dealers to maintain reasonably designed policies and procedures to protect customer information from security threats and unauthorized access. In February 2018, the SEC released its first formal cybersecurity guidance: Interpretive Guidance on Public Company Cybersecurity Disclosures.[53] Examples of alleged violations include:

- *SEC v. Sudhakar Reddy Bonthu*, No. 1:18-cv-03114 (June 28, 2018) (A few months later, the agency brought insider trading similar charges against a former Equifax software engineering manager engaged in insider trading for selling his Equifax put options before the company publicly disclosed a massive data breach affecting ~148 million U.S. consumers);
- *In the Matter of Altaba Inc., f/d/b/a Yahoo! Inc.*, 3-18448 (April 24, 2018) ($35 million fine against Yahoo! for misleading investors by failing to disclose a data breach that occurred in 2014);
- *SEC v. Jim Ying*, No. 1:18-cv-01069 (N.D. Ga. Mar. 14, 2018) (insider trading charges against a former Equifax chief information officer engaged in insider trading for selling his Equifax shares for almost $1 million before the company publicly disclosed a massive data breach).

iv - Consumer Protection

General Unfair and Deceptive Practices Cases. The FTC also uses its Section 5 authority to bring enforcement actions against tech companies like Google, Apple, Microsoft, HP, and Amazon for alleged

[53] SEC Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

unfair and deceptive advertising and marketing practices. Cases alleging unfair and deceptive practices include:

- *U.S., et al. v. Dish Network, LLC*, No. 3:09-cv-03073 (C.D. Ill. Aug. 10, 2017) (violated the FTC's Telemarketing Sales Rule, the TCPA, and state laws by initiating outbound phone calls to numbers on the Do Not Call Registry and assisting telemarketers with sufficient knowledge they were violating the law);
- *FTC v. Amazon.com, Inc.*, No. 2:14-cv-01038 (W.D. Wash. Dec. 22, 2016) (unfairly charged consumers for in-app purchases incurred by children without their parents' consent);
- *In the Matter of Google, Inc.*, Dkt. No. C-4499 (F.T.C. filed Sept. 4, 2014) (unfairly charged consumers for in-app purchases incurred by children without their parents' consent);
- *In the Matter of Apple, Inc.*, Dkt. No. C-3108 (F.T.C. Jan. 15, 2014) (unfairly charged consumers for in-app purchases incurred by children without their parents' consent)
- *U.S. v. Amazon.com, Inc.*, No. 1:13-cv-00002 (D.D.C. 2013) (offered for sale or selling falsely or deceptively labeled textile products);
- *FTC v. LifeLock, Inc.* (D. Ariz. Mar. 9, 2010) (among other things, falsely claimed its services offered absolute protection against identity theft);
- *In the Matter of CompuServe, Inc.*, Dkt. No. C-4105 (F.T.C. Sept. 23, 2003) (delayed delivery of $400 rebates to consumers who signed up for its internet service);
- *In the Matter of AOL, Inc.*, Dkt. No. C-4105 (F.T.C. Sept. 23, 2003) (continued to bill its internet service subscribers after they asked to cancel their subscriptions);
- *In the Matter of Gateway Corp.*, Dkt. No. C-4015 (F.T.C. June 24, 2001) (misrepresented that consumers would get one year of free or flat-fee internet access with the purchase of advertised computer models when, in fact, consumers incurred significant additional charges for such access);
- *In the Matter of Microsoft Corp.*, Dkt. No. C-4010 (F.T.C. April 3, 2001) and *In the Matter of Hewlett-Packard Co.*, Dkt. No. C-4009 (F.T.C. April 3, 2001) (misrepresented Pocket PC handheld computers came with built-in wireless internet and email access when in fact consumers had to purchase additional equipment to obtain such access).

Adware and Spyware. For over a decade, the FTC has brought enforcement actions against tech companies for installing adware and other software on consumers' computers and other products without their knowledge or consent. Examples alleging violations relating to adware and spyware include:

- *In the Matter of Lenovo, Inc.*, Dkt. No. C-4636 (F.T.C. Sept. 15, 2017) (sold laptops containing pre-installed adware that compromised consumer security);
- *FTC et al. v. Vizio, Inc. and Vizio Inscape Serv's., LLC*, No. 2:17-cv-00758 (D. N.J. Feb. 6, 2017) (installed software on its smart TVs to collect viewing data on 11 million consumer TVs without the consumers' knowledge or consent);

- *In the Matter of Zango, Inc. f/k/a 180 Solutions, Inc., et al.*, Dkt. No. 502-3130 (F.T.C. Mar. 9, 2007) (software company used unfair and deceptive methods to download adware and obstruct consumers from removing it in violation of federal law);
- *In the Matter of Advertising.com, Inc., et al.*, Dkt. No. 042-3196 (F.T.C. Aug. 3, 2005) (AOL subsidiary violated federal law by offering free security software to consumers but failing to adequately disclose that adware was bundled with that software).

Clear and Conspicuous Disclosures. The FTC has long regulated companies' advertising, marketing, promotional, and sales activities online. For example, the FTC requires tech companies to make online disclosures "clear and conspicuous," i.e., prominent, unavoidable, and placed in proximity to the relevant claim. In 2000, FTC staff released the *Dot Com Disclosures* guidance, in which it outlined how consumer protection laws apply to online marketing activities, what constitutes a clear and conspicuous disclosure online, and other requirements for online advertising and marketing claims (e.g., truthful and not misleading, substantiated, and not unfair). Staff updated the guidance in March 2013 to account for the increased use of smartphones and social media marketing in the digital age. More specifically, the FTC uses its Section 5 authority to regulate search engines, requiring tech companies to clearly and prominently distinguish paid search results from natural search results.[54] The FTC has levied section 5 charges against tech companies for failing to adhere to the principles outlined in the *.com Disclosures*. Cases alleging failure to provide clear and conspicuous disclosures include:

- *In the Matter of PayPal, Inc.*, Dkt. No. C-4651 (F.T.C. Feb. 27, 2018) (failed to provide clear and conspicuous disclosure of its privacy practices on its mobile payment service, Venmo);
- *FTC et al. v. Vizio, Inc. and Vizio Inscape Serv's., LLC*, No. 2:17-cv-00758 (D. N.J. Feb. 6, 2017) (touted its "Smart Interactivity" feature that "enables program offers and suggestions" but failed to inform consumers that the settings also enabled the collection of consumers' viewing data);
- *In the Matter of Turn, Inc.*, Dkt. No. C-4612 (F.T.C. Dec. 20, 2016) (requiring Turn to place a clear and conspicuous hyperlink on its site that consumers can click to opt-out of targeted advertising);
- *FTC v. Amazon.com, Inc.*, No. 2:14-cv-01038 (W.D. Wash. July 22, 2016) (finding a small hyperlink that said "In-App Purchasing" was not sufficiently obvious to alert consumers that they would be billed for in-app charges in an FTC case against Amazon for unauthorized billing practices);
- *U.S. v. InMobi*, No. 3:16-cv-3474 (N.D. Cal. June 22, 2016) (failed to clearly, completely, or accurately disclose all of its information collection and use practices).

[54] FTC Letter to Search Engines (June 24, 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ ftc-consumer-protection-staff-updates-agencys-guidance-search-engine-industryon-need-distinguish/130625searchenginegeneralletter.pdf.

Endorser Liability. The FTC investigates and brings cases under Section 5 for failure to provide adequate disclosures about material connections between endorsers and advertisers.[55] Cases alleging violations of endorsement guides include:

- *In the Matter of CSGOLOTTO, Inc., Trevor Martin, and Thomas Cassell*, Dkt. No. C-4632 (F.T.C. Nov. 29, 2017) (two social media influencers deceptively endorsed an online gambling service while failing to disclose that they jointly owned the company).
- *In the Matter of Warner Bros. Home Entmt. Inc.*, Dkt. No. C-4595 (F.T.C. Nov. 21, 2016) (failed to adequately disclose that it paid online influencers to post positive gameplay videos on YouTube and social media);
- *In the Matter of Machinima, Inc.*, No. C-4569 (F.T.C. Mar. 17, 2016) (deceptive advertising by online entertainment network for paying influencers to post YouTube videos endorsing Microsoft's Xbox One system and several games);
- *In the Matter of Deutsch LA, Inc.*, Dkt. No. C-4515 (F.T.C. Mar. 31, 2015) (Sony's advertising agency misled consumers by urging its employees to create awareness and excitement about a Sony gaming console without instructing them to disclose their connection to the advertising agency and Sony);
- *In the Matter of ADT LLC*, Dkt. No. C-4460 (F.T.C. June 24, 2014) (misrepresented that paid endorsements from safety and tech experts for online home security system who appeared as guests on news programs and talk shows were independent reviews).

Fintech. Federal agencies such as the Commodity Futures Trading Commission (CFTC), SEC, and FTC are increasingly focused on regulating emerging technologies like cryptocurrency and blockchain.

- Virtual currencies like Bitcoin and Etherium are commodities subject to CFTC authority under the Commodity Exchange Act. The CFTC has, among other things, taken action against unregistered Bitcoin futures exchanges, issued guidance on derivative markets, and addressed a virtual currency ponzi scheme.[56] Cases alleging violations include:
    - *CFTC v. 1Pool Ltd.*, No. 1:18-cv-2243 (D.D.C. Mar. 4, 2019) ($990,000 fine from 1pool Ltd. and its CEO for illegally offering retail commodity transactions that were margined in Bitcoin, failing to register as a futures commission merchant, and failing to meet its supervisory duties by not having anti-money laundering procedures in place);
    - *In the Matter of Joseph Kim*, No. 19-02 (C.F.T.C. Oct. 29, 2018) ($1.1 million fine from a trader at a proprietary trading firm who operated a fraudulent Bitcoin and Litecoin scheme that resulted in more than $1 million in losses);
    - *CFTC v. Gelfman Blueprint, Inc.*, No. 17-cv-07181 (S.D.N.Y. Oct. 8, 2018) ($2.5 million penalty and restitution for operating a Bitcoin ponzi scheme in which $600,000 was fraudulently solicited from at least 80 consumers);

[55] 16 C.F.R. Part 255 (Endorsement Guides).

[56] CFTC Press Release, *CFTC Staff Issues Advisory for Virtual Currency Products* (May 21, 2018), https://www.cftc.gov/PressRoom/PressReleases/7731-18.

- *CFTC v. My Big Coin Pay, Inc. et al.*, No. 1:18-cv-10077 (D. Mass. Jan. 16, 2018) (commodity fraud and misappropriation for soliciting customers for a virtual currency scam);
- *In the Matter of Coinflip, Inc.*, No. 15-29 (C.F.T.C. Sept. 17, 2015) (company operated an online facility offering to connect buyers and sellers of bitcoin option contracts without complying with the Commodity Exchange Act and CFTC Regulations).

- Using its Cyber Unit focused on misconduct involving distributed ledger technology and initial coin offerings (ICOs), the SEC has brought a number of enforcement actions concerning ICOs and token issuers for violations of federal securities laws. Actions alleging violations include:
  - *SEC v. Arisebank, Jared Rice Sr., and Stanley Ford*, No. 3:18-cv-00186 (N.D. Tex. Dec. 11, 2018) ($2.7 million in disgorgement and civil penalties for offering and selling unregistered investments in fraudulent ICO's purported "AriseCoin" cryptocurrency).
  - *In the Matter of Paragon Coin, Inc.*, No. 3-18897 (S.E.C. Nov. 16, 2018) (illegally unregistered securities);
  - *In the Matter of Carriereq, Inc.*, No. 3-18898 (S.E.C. Nov. 16, 2018) (illegally unregistered securities);
  - *SEC v. Plexcorps, Dominic Lacroix, and Sabrina Paradis-Royer*, No. 17-cv-7007 (E.D.N.Y. Dec. 1, 2017) (emergency asset freeze to halt ICO fraud that purportedly duped thousands of investors out of $15 million).
- The FTC has also levied section 5 claims alleging deception in this area. For example:
  - *FTC v. Thomas Dluca*, No. 0:18-cv-60379 (S.D. Fla. Mar. 12, 2018) (chain referral scheme that promised big rewards for a small payment of Bitcoin or Litecoin);
  - *TC v. BF Labs, Inc.*, No. 4:14-cv-00815 (W.D. Mis. Feb. 18, 2016) (charged consumers thousands of dollars for its Bitcoin mining machines then failed to deliver the computers or delivered machines that were practically useless);
  - *FTC v. Equiliv Investments and Ryan Ramminger*, No. 142-3144 (F.T.C. June 9, 2015) (smartphone app developer lured customers into downloading its "rewards app" that loaded consumers' phones with malicious software to mine virtual currencies).

B - State Privacy and Data Security Protections

i - Privacy

- State laws prohibiting unfair and deceptive acts or practices, often called "little FTC Acts," and other consumer protection laws give all 50 states and the District of Columbia similar enforcement power as the FTC. Further, state laws like CalOPPA and California's "Shine the Light" law mandate privacy disclosures and give consumers specific privacy rights to know and, in some cases, consent to how their data is being shared. Individual states and multi-state groups often take action against tech companies for allegedly violating state unfair and deceptive practices laws, customer records laws, eavesdropping laws, and other state consumer protection laws.

State laws prohibiting unfair and deceptive acts or practices, often called "little FTC Acts," and other consumer protection laws give all 50 states and the District of Columbia similar enforcement power as the FTC.

Examples of state actions alleging privacy violations include:

- In 2018, the New York attorney general obtained a $4.5 million civil penalty against Oath f/k/a AOL for conducting ad auctions for targeted ads on children's websites in violation of COPPA;[57]
- *District of Columbia v. Facebook, Inc.*, 2018 CA 008715 B (D.D.C. Dec. 2018) (sued for violating DC law by misleading users about the security of their data, failing to properly monitor third party apps' use of data, making it difficult for users to control data settings for apps, failing to disclose the Cambridge Analytica breach, failing to ensure users' improperly obtained data was deleted, and failing to inform consumers that some companies could override data privacy settings);
- *New Mexico v. Tiny Lab Prod. et al.*, No. 6:18-cv-00854 (Sept. 2018) (suing Twitter, Google, and other companies for violating COPPA and New Mexico's consumer protection act by allegedly collecting and using children's personal data for targeted advertising);
- *California v. Lenovo (US) Inc.*, No. BC-674647 (Cal. Sup. Ct. Sept. 2017) ($3.5 million to settle multistate action alleging violations of state consumer protection laws for pre-installing adware on laptops sold to consumers);
- *California v. Comcast et al.*, No. RG15786197 (Cal. Sup. Ct. 2015) ($33 million for violating California law by posting online names, phone numbers, and addresses of customers who paid for unlisted phone services);
- *California v. Comcast Cable Communications, LLC* (Cal. Sup. Ct. Dec. 2015) (violated California law by disposing of customer records without erasing or otherwise modifying the personal information in those records);
- *California v. Houzz*, No. 115-cv-286406 (Cal. Sup. Ct. Oct. 2015) (online home design platform violated California eavesdropping and wiretapping laws by secretly recording its customers' phone calls for training and quality assurance purposes without obtaining their consent);
- *In the Matter of Sirius XM Radio*, Ohio Office of the Attorney General Dkt. No. 413647 (Dec. 2014) (settling allegations brought by 46 state AGs that the company violated state consumer protection laws by, among other things, ignoring customers'

[57] NYAG Press Release, A.G. Underwood Announces Record COPPA Settlement with Oath - Formerly AOL - For Violating Children's Privacy (Dec. 4, 2018), https://ag.ny.gov/press-release/ag-underwood-announces-record-coppa- settlement-oath-formerly-aol-violating-childrens.

cancellation requests and renewing their contracts and increasing their rates without their knowledge or consent);

- In 2014, Snapchat paid $100,000 to settle a state consumer protection and COPPA action brought by the Maryland attorney general for misrepresenting the temporary nature of snaps and collecting personal information from children without verifiable parental consent;[58]
- In 2013, Google paid $7 million to settle a multistate action alleging unauthorized collection of data from unsecured wireless networks while taking photos for the Street View service;[59]
- *California v. HP*, No. 1:06-cv-076081 (Cal. Sup. Ct. 2006) ($14.5 million settlement for violations of state constitutional right to privacy by obtaining confidential phone records and other personal data without notice and consent).

- 39 states have passed student privacy laws that, among other things, restrict tech companies' use of student data and give students control over their data and the right to know how it is being used. Many states model their student privacy laws after California's Student Online Personal Information Protection Act (SOPIPA),[60] which prohibits tech companies from knowingly engaging in targeted advertising to students, using covered information to amass a profile about a K-12 student, and selling or disclosing a student's covered information.

  A few states, including California, have passed laws that regulate the activities of online service providers and cloud computing services. Other states have enacted laws that impose security requirements for student data, or require service providers to be subject to specific contractual requirements, such as use and disclosure restrictions.

39 states have passed student privacy laws that, among other things, restrict tech companies' use of student data and give students control over their data and the right to know how it is being used.

For example:

- Colorado requires education service provider contracts to include express provisions mandating safeguards for student data privacy and security, prohibiting student data

[58] MDAG Press Release, Attorney General Gansler Secures Settlement from Snapchat, Inc. (June 12, 2014) http://www.marylandattorneygeneral.gov/Press/2014/061214.pdf.

[59] NYAG Press Release, A.G. Schneiderman Announces Multistate Settlement with Google For Violating Privacy Rights (Mar. 12, 2013), https://ag.ny.gov/press-release/ag-schneiderman-announces-multistate-settlement-google- violating-privacy-rights.

[60] SB 1177.

from being used for purposes other than those provided in the contract, and prohibiting further disclosure and use for commercial purposes, among other things;[61]

- Connecticut prohibits operators from engaging in targeted advertising, using student information and other data for purposes other than "school purposes," selling, renting or trading student information, and disclosing student information unless certain exceptions apply;[62]
- Delaware prohibits service providers from engaging in targeted advertising, building student profiles, selling student data, and disclosing student data unless certain exceptions apply;[63]
- Georgia prohibits operators from knowingly engaging in behaviorally targeted advertising, using information for profiling, selling student data, and disclosing student data without consent, among other things;[64]
- Washington requires service providers to provide clear privacy policies and have a security plan, and prohibits the sale of student information for targeted advertising, creating a profile, or any other purpose without consent.[65]

- Three states have passed laws that regulate the collection, use, and disclosure of biometric information. The Illinois Biometric Information Privacy Act (BIPA)[66] regulates tech companies' collection, use, and disclosure of biometric data (i.e., retina and iris scans, fingerprints, voiceprints, and hand or face geometry). Private litigants can enforce this law and obtain statutory damages of $1,000 for each negligent violation and $5,000 for each intentional or reckless violation. Texas has a biometrics law that requires, among other things, notice and opt-in consent to collect and disclose biometric identifiers (defined to include retina or iris scans, fingerprints, and records of hand or face geometry).[67] It is enforced by the attorney general, who can obtain civil penalties of up to $25,000 per violation. Washington also passed a biometric privacy law that is enforced by the attorney general under the state's consumer protection act and prohibits enrolling a biometric identifier in a database for commercial purposes without notice and consent, among other things.[68] Private litigants have been especially active in enforcing these laws. ***See section I.C for more details.***

---

[61] Colo. Rev. Stat. § 22-16-104.

[62] Conn. Gen. Stat. Ann. §§10-234aa to 10-234dd.

[63] 14 Del. C. §§ 8101a to 8106a.

[64] Ga. Code. Ann. §§ 20-2-660 to 20-2-668.

[65] RCW § 28A.604.010 to 28A.604.903.

[66] 740 ILCS 14/1 *et seq.*

[67] Texas Bus. & Com. Code § 503.001.

[68] RCW §§ 19.375.1010 to 19.375.900.

ii - Data Security

- All 50 states have enacted data breach notification laws that impose increasingly strict requirements on tech companies to promptly notify consumers of data breaches and/or unauthorized access to data.[69] California and other states regularly expand the definition of covered "personal information," most recently to include online account login credentials. Over a dozen of these laws contain a private right of action. For example:
    - States including California, Florida, Illinois, Nebraska, and South Dakota require notification if an email address and password or security question that would permit access to an online account is breached;[70]
    - States including Nebraska and Nevada require notification if a first name or first initial and last name plus unique electronic identification number or routing code and password, security code, or access code is breached;[71]
    - States including Illinois, Iowa, Nebraska, North Carolina, Oregon, South Dakota, Wisconsin, and Wyoming require notification if first name or first initial and last name plus unique biometric data is breached;[72]
    - States including Alaska, California, Illinois, and Massachusetts, among others, permit a private right of action in the event of a breach.[73]
- Approximately 30 states have data disposal laws that require tech companies to securely dispose of personal information.[74] Some states, like California, define personal information broadly to include any information that can be associated with a particular individual, such as name, signature, address, physical characteristics, and phone number.[75]

Approximately 30 states have data disposal laws that require tech companies to securely dispose of personal information.

[69] *See, e.g.*, Cal. Civ. Code §§ 1798.80-82; M.G.L.A. 93H §§ 1 to 6.

[70] Cal. Civ. Code §§ 1798.80-82; Fla. Stat. § 501.171; 815 ILCS 530/10; Neb. Rev. St. §§ 87-801-807; S.D. § 22-40.

[71] Neb. Rev. St. §§ 87-801-807; N.R.S. §§ 603A.010-.040.

[72] 815 ILCS 530/10, Iowa Code § 715C.2; Neb. Rev. St. §§ 87-801-807; N.C.G.S.A. §§ 75-60-66; Or. Rev. Stat. §§ 646A.600-.628; S.D. § 22-40; Wis. Stat. § 134.98; Wyo. Stat. § 40-12-501 *et seq.*

[73] *See, e.g.*, Alaska Stat. §§ 45.48.500 *et seq.*; Cal. Civ. Code §§ 1798.80, 81, and 84; 815 ILCS 530/10; Mass. Gen. Laws Ch. 931 § 2.

[74] *See, e.g.*, Alaska Stat. §§ 45.48.500 *et seq.*; Ark. Code §§ 4-110-103-104; Colo. Rev. Stat. § 6-1-713; Fla. Stat. § 501.171(8); Ga. Code § 10-15-2; Mass. Gen. Laws Ch. 931 § 2; N.J. Stat. § 57-12C-3; Va. Code § 2.2-2009(F); Wash. Rev. Code § 19.215.020.

[75] *See, e.g.*, Cal. Civ. Code §§ 1798.80, 81, and 84; Conn. Gen. Stat. Ann. §§ 42-471a; Del. Code tit. 6,§§ 5001C-5004C; Fla. Stat.§ 501.171; Haw. Rev. Stat. §§ 487R-1-3; 815 ILCS 530/5 and 530/40; M.G.L. Ch. 93I, §§ 1-2; M.C.L. §§ 445.63 and 445.72a.

- A few states, such as Alaska, also require companies to adopt written data disposal policies.[76]
- Some states, such as California, Maryland, and Oregon, require companies that disclose personal information to third parties to impose reasonable data security obligations on them.[77]
- Approximately 20 states have enacted laws that prohibit tech companies from distributing malicious software or adware to consumers.[78] For example:
    - California prohibits copying computer software onto California consumers' computers and using that software to, among other things, modifying the computer's settings through intentionally deceptive means, collecting personal data through intentionally deceptive means, and intentionally misrepresenting that software will be uninstalled or disabled by an authorized user's action;[79]
    - New York criminalizes the unauthorized access to computers, computer services, and computer networks without authorization computer trespass, computer tampering, and other related conduct.[80]
- State student privacy laws, like California's SOPIPA, require tech companies to maintain reasonable security practices, protect student information, and delete information upon the school or school district's request. ***See section 1.A.i for more details.***
- State attorneys general have investigated and taken action against tech companies for violating state unfair and deceptive practices laws for failing to prevent alleged data breaches and other security related violations. Examples of cases alleging such violations include:
    - *Arizona et al. v. Med. Informatics Eng., Inc.*, No. 3:18-cv-969 (N.D. Ind. 2019) ($900,000 to settle multistate action for medical software provider's violations of HIPAA, state consumer protection laws, state data breach laws, and state personal information protection acts);
    - *Iowa ex rel. Thomas J. Miller, Attorney General of Iowa v. Uber Tech., Inc.*, Equity No. _____ (Iowa Dist. Ct. for Polk Cty. Sept. 2018) (settling claims brought by all 50 state attorneys general over a 2016 data breach for $148 million);
    - *In the Matter of Adobe Systems, Inc.* (Nov. 2016) (settling allegations brought by 15 state AGs for violating state data breach notification and consumer protection laws by failing to employ reasonable security measures to protect its systems and failing to promptly detect and respond to unauthorized activity on its network);

[76] *See, e.g.*, Alaska Stat. §§ 45.48.500 *et seq.*;

[77] Cal. Civ. Code § 1798.81.5; Md. Code Ann. Com. Law § 14-3503; Or. Rev. Stat. § 646.622(2)(d).

[78] *See, e.g.*, CAL. BUS. & PROF. CODE §§ 22947-22947.6; 720 ILCS 5/17-52; N.Y. Penal Law § 156.

[79] Cal. Bus. & Prof. Code §§ 22947-22947.6.

[80] N.Y. Penal Law §§ 156.00 *et seq.*

- *In the Matter of State of Texas and PayPal, Inc.* (May 2016) (violated the Texas Deceptive Trade Practices Act by, among other things, using consumers' phone contacts without clearly disclosing how their transactions and interactions would be shared).

C - Private Litigants Enforcing Consumer Rights

- Private parties routinely bring actions related to companies' data handling practices under state and federal laws. Plaintiffs have brought numerous cases under state and federal privacy and data security statutes. Plaintiffs lawyers are particularly eager to bring class actions against large tech companies using laws that contain statutory damages, such as the Illinois Biometric Information Privacy Act ($1,000 for each negligent violation; $5,000 for each intentional or reckless violation) to secure significant financial settlements.

Private litigants have recoupled more than $40mill through lawsuits under existing privacy laws.

- Examples of cases alleging privacy and data security violations include, among others:
- *In re: Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-md-02752, Dkt. 369 (N.D. Cal. 2019) (proposing $117 million settlement in multidistrict action for historic data security breach);
- *Manigault-Johnson v. Google, LLC, Alphabet, Inc, and YouTube, LLC*, No. 2:18-cv-01032 (D.S.C. 2018) (alleging Google violated the common law and California Constitutional Right to Privacy by collecting and sharing children's personal information through the YouTube platform in violation of COPPA);
- *Marc Opperman, et al. v. Kong Tech., Inc., et al.*, No. 13-cv-00453 (N.D. Cal. 2018) ($5.3 million to settle class allegations that the companies uploaded users' address book data without their knowledge or consent);
- *In re Lenovo Adware Litig.*, No. 15-md-02624 (N.D. Cal. 2018) ($8.3 million settlement for pre-installing adware on computers sold to consumers);
- *Patacsil v. Google, Inc.*, No. 3:18-cv-05062 (N.D. Cal. 2018) (alleging Google violated the California Invasion of Privacy Act, California Constitutional Right to Privacy, and common law right to privacy by tracking users' location without their consent);
- *In re: Facebook Privacy User Profile Information*, MDL No. 2843 (N.D. Cal. 2018) (alleging Facebook violated various statutes and state common law by exfiltrating without authorization user data for Cambridge Analytica's targeted ads during the 2016 presidential campaign);
- *Rosenbach v. Six Flags Ent. Corp.*, No. 2-17-0317 (Ill. App. Dec. 21, 2017) (alleging the company violated BIPA by fingerprinting plaintiffs without notice and consent);
- *Matera and Rashkis v. Google, Inc.*, No. 5:15-cv-04062 (N.D. Cal. 2017) ($2.2 million settlement for violating the California Invasion of Privacy Act and Electronic

Communications Privacy Act by applying automated processing to intercept, extract, read, and use the contents of non-Gmail users' emails for advertising purposes);

- *Monroy v. Shutterfly, Inc.*, No. 1:16-cv-10984 (N.D. Ill. 2017) (denying Shutterfly's motion to dismiss on the basis that the identifiers at issue were not specifically listed in the statute);
- *In re: Apple Inc. Device Performance Litigation*, No. 5:18-md-02827 (N.D. Cal. 2017) (suing Apple for fraud and unfair and deceptive trade practices for allegedly integrating performance degrading features into iOS updates);
- *Dancel v. Groupon, Inc.*, No. 1:18-cv-2027 (Ill. Cir. Ct. 2016) (alleging violation of Illinois Right of Publicity Act based on collection of Groupon users' Instagram photos in order to advertise on Groupon);
- *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016) (alleging Facebook violated BIPA when it launched its "Tag Suggestions" feature, which used facial recognition algorithms to deliver suggested names of individuals in photos);
- *Rivera et al. v. Google, LLC*, No. 1:16-cv-02714 (N.D. Cal. 2016) (alleging Google violated BIPA by collecting, storing, and using biometric information, including face-geometry scans, without first obtaining consent or providing required disclosures);
- *Norberg v. Shutterfly, Inc. et al.*, No. 1:15-cv-05351 (N.D. Ill. 2015) (alleging Shutterfly violated BIPA by creating and storing faceprints to identify individuals in photos without consent);
- *In re: Vizio Inc. Consumer Privacy Litigation*, No. 8:16-ml-02693 (C.D. Cal. 2015) ($17 million settlement for violations of the Video Privacy Protection Act and ECPA by collecting consumers' personal video-viewing habits and selling to data brokers without consumer consent);
- *Norcia et al. v. Samsung Telecomms. America, LLC*, No. 3:14-cv-000582 (N.D. Cal. 2014) (alleging Samsung adjusted processing speeds during benchmark tests in an effort to deceive consumers and asserting claims for violation of the California Consumer Legal Remedies Act, unfair and deceptive business practices, false advertising, and fraud);
- *Halpain v. Adobe* (N.D. Cal. 2013) (alleging unfair and deceptive trade practices, violations of California's data breach statute and common law claims in the wake of data breaches for failure to properly secure and protect users' personal information);
- *In re: Netflix Privacy Litig.*, No. 5:11-cv-00379 (Sept. 5, 2012) ($9 million to settle class action claims under the Video Privacy Protection Act);
- *In re: Facebook Internet Tracking Litig.*, 844 F. Supp. 2d 1374 (J.P.M.L. 2012) (violated the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and state common law by improperly tracking users' internet activity after they had logged out of their accounts).

- The plaintiffs' bar regularly brings privacy claims forward under contract and fraud theories. It also continues to innovate privacy claims premised on other common law theories. Recent examples include the following:

- *Rushing v. Disney Co. et al.*, No. 3:17-cv-04419 (N.D. Cal. Aug. 3, 2017) (alleging Disney unlawfully collected personal information from children based on a theory of intrusion upon seclusion);
- *In re: Nickelodeon Consumer Privacy Litigation*, No. 15-cv-1441 (3rd Cir. 2016) (alleging Viacom and Google inadvertently swept up information from children under the theory of "intrusion upon seclusion"—traditionally a privacy tort reserved for the physical realm);
- *Henson v. Turn*, No. 4:15-cv-01497 (N.D. Cal. 2015) (alleging Turn, a third party ad platform, illegally placed cookies on Verizon users' mobile browsers under a trespass to chattels theory).

D - Industry Self-Regulation of Privacy and Advertising

- Self-regulatory programs provide robust protections for consumers and are aggressively enforced by the FTC, particularly in the advertising space. Companies that fail to abide by their commitments to these codes of conduct are subject to disciplinary actions by the programs and enforcement by the FTC for deception. For example:
  - The Council of the Better Business Bureau's Advertising Self-Regulatory Council (ASRC) administers a number of self-regulatory programs for hundreds of companies (including many in tech) that set advertising standards (such as truth and accuracy standards) for national advertisers. The ASRC reviews member companies' compliance with these standards, refers select cases to regulators for further investigation or inquiry, and provides a dispute resolution mechanism for consumers and companies to raise possible compliance issues:
    - The Children's Advertising Review Unit (CARU)[81] is an investigative unit of the ASRC that develops policies and procedures for child-directed advertising and promotional materials. It also operates a safe harbor program to assist companies in complying with COPPA and its guidelines. CARU monitors, reviews, and evaluates child-directed advertising and online privacy practices that may affect children, and refers cases involving misleading, inaccurate, or inconsistent advertising practices to regulators when companies fail to comply with its recommendations. For example:
      - In May 2019, Facebook updated its mechanism for blocking users under 13 from signing up for its mobile app in response to a CARU recommendation;[82]

[81] Children's Advertising Review Unit, https://asrcreviews.org/about-caru/.

[82] BBB NP Press Release, CARU to Facebook: Improve Mechanisms for Blocking Under-13 Users, May 1, 2019, *available at* https://asrcreviews.org/caru-to-facebook-improve-mechanisms-for-blocking-under-13-users-facebook-agrees-to-place-age-gating-mechanisms-in-mobile-app-to-prevent-children-from-falsifying-age/.

- In April 2018, CARU referred Musical.ly to the FTC after it refused to comply with CARU's COPPA recommendations.[83] In February 2019, Musical.ly settled with the FTC for $5.7 million, the largest civil penalty the FTC has ever imposed in a COPPA case;[84]
- In May 2011, Microsoft agreed to modify its advertising of and disclosures relating to a video game played by children in response to a CARU recommendation;[85]
- In 2009, Google agreed to age screen future Gmail users during the registration process in response to a CARU recommendation.[86]

■ The Electronic Retailing Self-Regulation Program (ERSP)[87] monitors and reviews advertising representations of participating telemarketers and live seminar providers for coaching and mentoring services, and of lead generation advertising disseminated by non-participating companies that may impact the coaching and mentoring industry. Participating companies are provided with written assessments of their telemarketing and live seminar practices and follow-up compliance reviews. ERSP reviews that do not yield recommendations that claims be modified or discontinued do not guarantee that regulators or other self-regulatory programs will not investigate or file actions against participating companies. ERSP refers compliance investigations to the FTC when companies do not respond to its inquiries or otherwise fail to participate in its self-regulatory process.[88]

■ The National Advertising Division (NAD)[89] reviews national advertising and sets standards for truth in advertising across industries. NAD opens cases against companies relating to their advertising practices either on its own initiative or in response to complaints and challenges filed by consumers and other companies. NAD gives advertisers the opportunity to voluntarily participate in self-

---

[83] BBB NP Press Release, CARU Refers Musical.ly to FTC After App Operator Declines to Comply with CARU's Privacy Recommendations, April 14, 2018, *available at* https://asrcreviews.org/caru-refers-musical-ly-to-ftc-after-app-operator-declines-to-comply-with-carus-privacy-recommendations/.

[84] *U.S. v. Musical.ly*, No. 2:19-cv-01439 (C.D. Cal. Feb. 27, 2019).

[85] CARU Press Release, CARU Recommends Microsoft Modify Kinectimals Advertising To Better Disclose Material Information; Company Does So, May 11, 2011, *available at* https://asrcreviews.org/caru-recommends-microsoft-modify-kinectimals-advertising-to-better-disclose-material-information-company-does-so/.

[86] CARU Press Release, CARU, Google Collaborate to Ensure Children's Privacy Protection On Gmail.com, Aug. 11, 2009, *available at* https://asrcreviews.org/caru-google-collaborate-to-ensure-childrens-privacy-protection-on-gmail-com/.

[87] Electronic Retailing Self-Regulatory Program, https://asrcreviews.org/about-ersp/.

[88] *See, e.g.*, BBB NP Press Release, ERSP Refers Advertising for Alo Yoga to FTC for Further Review, Oct. 18, 2018, *available at* https://asrcreviews.org/ersp-refers-advertising-for-alo-yoga-to-ftc-for-further-review/.

[89] National Advertising Division, https://asrcreviews.org/how-nad-works/.

regulation in response to these cases, and refers companies that fail to cooperate with the NAD or follow its recommendations to the FTC and other regulatory agencies.[90] For example:

- In May 2019, Verizon agreed to modify or discontinue its claims that it is the "Best Network" and "Best Unlimited," and that it offers the "most reliable 4G LTE network" and the "best network for streaming" in response to NAD's recommendation;[91]
- In March 2019, MLW Squared, Inc. agreed to modify or discontinue claims regarding its Tri-Verified influencer marketing platform;[92]
- In November 2018, NAD referred LG Electronics to the FTC for further review of its advertising claims to "perfect black" and "infinite contrast."[93]
- In February 2018, NAD referred T-Mobile to the FTC and FCC for further review of its advertising after it declined to participate in a NAD proceeding;[94]
- In January 2018, NAD referred StubHub to the FTC for further review of its pricing claims after it declined to comply with NAD's recommendations to more clearly disclose additional taxes and fees that apply to tickets purchased on the ticket exchange platform.[95]

■ The National Advertising Review Board (NARB)[96] is the appellate body of the ASRC that reviews NAD and CARU decisions appealed by target companies.

---

[90] *See, e.g.*, BBB NP Press Release, NAD Refers T-Mobile Advertising to FTC, FCC for Further Review After Advertiser Declines to Participate; Claims Challenged by AT&T, Feb. 16, 2018, *available at* https://asrcreviews.org/nad-refers-t-mobile-advertising-to-ftc-fcc-for-further-review-after-advertiser-declines-to-participate-claims-challenged-by-att/.

[91] BBB Press Release, NAD Finds Verizon's Ranked #1 by RootMetrics Claims Supported; Recommends Verizon Modify, Discontinue Unqualified "Best Network" and Other Claims, May 7, 2019, *avaialble at* https://asrcreviews.org/nad-finds-verizons-ranked-1-by-rootmetrics-claims-supported-recommends-verizon-modify-discontinue-unqualified-best-network-and-other-claims/.

[92] BBB Press Release, NAD Recommends Discontinuance And Modification of Certain Claims By MLW Squared, Inc. For Ti-Verified Influencer Marketing Platform, Mar. 25, 2019, *available at* https://asrcreviews.org/nad-recommends-discontinuance-and-modification-of-certain-claims-by-mlw-squared-inc-for-tri-verified-influencer-marketing-platform/.

[93] BBB NP Press Release, NAD Refers Advertising Claims by LG Elecs. To FTC for Further Review; NAD Declines to Reopen LG Case Under New Evidence Rules, Oct. 19, 2018, *available at* https://asrcreviews.org/nad-refers-advertising-claims-by-lg-electronics-to-ftc-for-further-review-nad-declines-to-reopen-lg-case-under-new-evidence-rules/.

[94] BBB Press Release, NAD Refers T-Mobile Advertising to FTC, FCC, for Further Review After Advertiser Declines to Participate; Claims Challenged by AT&T, Feb. 16, 2018.

[95] BBB Press Release, NAD Refers StubHub Pricing Claims to FTC for Further Review After Advertiser Declines to Comply with NAD Decision on Disclosures, Jan. 16, 2018, *available at* https://asrcreviews.org/nad-refers-stubhub-pricing-claims-to-ftc-for-further-review-after-advertiser-declines-to-comply-with-nad-decision-on-disclosures/.

[96] Advertising Self-Regulatory Council, http://www.asrcreviews.org/.

- Industry groups like the Network Advertising Initiative (NAI)[97] and Digital Advertising Association (DAA)[98] operate self-regulatory programs that require members to provide notice and choice in connection with interest based advertising, retargeting, and similar practices.
    - The NAI enforces its standards through ongoing member monitoring; annual compliance reviews; and, where necessary, sanctions imposed by the NAI Board of Directors. The DAA program is enforced by the ASRC's Online Accountability Program. Nearly a hundred companies are members of the NAI self-regulatory program and over a hundred companies are members of the DAA self-regulatory program, including some of the largest tech companies like Facebook, Google, HP, Microsoft, Netflix, Oath, Oracle, and Pinterest.
- The Future of Privacy Forum and The Software & Information Industry Association operate the Student Privacy Pledge, where tech companies may sign up to commit to safeguarding student privacy.[99] Companies including Google, Apple, Microsoft, AT&T, Canvas, and Lexicon Technologies have signed the Pledge.

- The FTC has investigated and/or taken action against tech companies based on ASRC referrals, some of which have resulted in significant penalties. Examples include:
    - In 2013, the NAD referred Oracle's advertising claims to the FTC after determining that "the company [did] not ma[ke] a good faith effort to comply with the recommendations of previous NAD decisions."[100]
    - In 2004, UMG Recordings, Inc. and Bonzi Software, Inc. agreed to pay $400,000 and $75,000 in civil penalties, respectively, to settle COPPA allegations brought by the FTC based on CARU referrals.[101]
- In the course of its investigations, the FTC also reviews compliance with relevant self-regulatory codes:
    - In 2012, Google paid $22.5 million to settle FTC charges that it violated an earlier FTC privacy settlement by misrepresenting its placement of cookies depending on the settings of Apple's Safari browser. The FTC complaint also alleged that Google

---

[97] Network Advertising Initiative, https://www.networkadvertising.org/.

[98] Digital Advertising Alliance, https://digitaladvertisingalliance.org/.

[99] Student Privacy Pledge, https://studentprivacypledge.org/.

[100] ASRC Press Releases, NAD Refers Advertising by Oracle to FTC After Company Repeatedly Fails to Comply with NAD Recommendations (Aug. 1, 2013), http://www.asrcreviews.org/nad-refers-advertising-by-oracle-to-ftc-after- company-repeatedly-fails-to- comply-with-nad-recommendations-2/.

[101] FTC Press Release, UMG Recordings, Inc. to Pay $400,000, Bonzi Software, Inc. To Pay $75,000 to Settle COPPA Civil Penalty Charges (Feb. 18, 2004), https://www.ftc.gov/news-events/press-releases/2004/02/umg- recordings-inc-pay-400000-bonzi-software-inc-pay-75000-settle.

misrepresented the extent to which it honored NAI's code of conduct.[102] In a blog post released shortly after the settlement was announced, the FTC warned businesses that "[m]embership in self-regulatory programs is your call, but once you advertise your adherence to an industry code, live up to its terms."[103]

2 - PLATFORM RESPONSIBILITY

A - Content Liability

Tech platforms face civil and criminal liability for content on their platforms under a host of laws, including federal copyright laws and obscenity laws. While Section 230 of the Communications Decency Act ("CDA") provides an exemption to tech platforms from liability for many types of user-generated content that they host, the platforms still face various forms of liability and regulatory pressures.

While Section 230 of the Communications Decency Act ("CDA") provides an exemption to tech platforms from liability for many types of user-generated content that they host, the platforms still face various forms of liability and regulatory pressures.

i - Federal copyright laws and intermediary liability

- Federal copyright laws impose direct and secondary liability on platforms that infringe copyright, and do so under a strict liability scheme. Corporate officers who control the infringing activity are individually liable along with the company. The CDA does not exempt tech platforms from federal IP law.[104]
    - In *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005), the Supreme Court held that a tech company that distributed peer-to-peer technology facilitating copyright infringement was subject to injunctive relief and monetary damages under an inducement theory.
    - In *American Broadcasting Company v. Aereo, Inc.*, 573 U.S. 431 (2014), the Supreme Court held a tech company liable for providing the means by which rights holder's TV broadcast programming was made available over the Internet.
    - In *UMG Recording Inc. et al. v. Escape Media Group, Inc. et al.*, No. 11-08407 (S.D.N.Y. 2015), music site Grooveshark shut down before the amount of damages was

[102] FTC Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[103] FTC Business Blog, Track afield: What the FTC's Google case means for your company (Aug. 13, 2012), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2012/08/track-afield-what-ftcs-google-case-means-your-company.

[104] 47 U.S.C. § 230(e)(2).

determined in a case against it where liability could have reached as high as $736 million in statutory damages.

- Federal copyright laws provide an arsenal of remedies to rights holders whose works have been infringed including temporary and permanent injunctive relief, recovery of the rights holder's actual damages plus the infringer's profits (avoiding double counting), and unique-in-the-world statutory damages with a minimum award of $750 and a maximum award of $30,000 per work, without the need to show any actual harm. Statutory damage awards are aggregated per work and may run into the hundreds of millions of dollars against any given infringer.
- Platforms in particular have been subject to a detailed regulatory regime since the 1998 Digital Millennium Copyright Act ("DMCA") also imposes restrictions in its notice and takedown requirements in order for platforms to enjoy limited safe harbors. The DMCA creates mechanisms for copyright owners to identify and request the takedown of content from Internet services, and those owners can bring infringement cases when tech companies are not complying with DMCA requirements of expeditiously taking down content after receiving such notifications, or for not having a policy dealing with repeat infringers.
    - In *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 293 (4th Cir. 2018), an ISP was found to have failed to implement its repeat infringer policy in any consistent or meaningful way, and thus disqualified from the DMCA's safe harbors. The Second and Seventh Circuits had similarly already so held, *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 83 (2d Cir. 2016); *In re Aimster Copyright Litig.*, 252 F.Supp.2d 634, 659 (N.D. Ill. 2002), aff'd, 334 F.3d 643 (7th Cir. 2003).

ii - Federal speech intermediary liability

- Tech platforms risk both civil and criminal liability for content on their platforms, including when they provide tools for third party companies to deliver advertisements to consumers.
- Specifically, tech platforms face liability when they benefit from allowing companies to disseminate harmful advertisements on their platforms. For example, in 2011, Google paid $500 million to settle allegations that it allowed online Canadian pharmacies to place advertisements through its Adwords program that targeted U.S. consumers and resulted in the unlawful importation of prescription drugs into the U.S.[105]
- Congress also recently passed the Stop Enabling Sex Traffickers Act (SESTA) and Allow States and Victim to Fight Online Sex Trafficking Act (FOSTA)[106] FOSTA-SESTA was designed to help combat online sex trafficking. Specifically, FOSTA-SESTA clarifies that Section 230 "does not prohibit the

[105] DOJ Press Release, Google Forfeits $500 Million Generated by Online Ads & Prescription Drug Sales by Canadian Online Pharmacies (Aug. 24, 2011), *available at* https://www.justice.gov/opa/pr/google-forfeits-500-million-generated-online-ads-prescription-drug-sales-canadian-online.

[106] Pub. L. No: 115-164 (2018).

enforcement . . . of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking" against tech platforms.[107]

- It expands the scope of the federal sex trafficking laws to make the mere intentional "facilitat[ion]" of prostitution by an online service provider a federal crime.[108]
- Although the pre-amendment Section 230 would have permitted the federal government to criminally charge a technology company with sex trafficking (albeit under the narrower pre-amendment definition of that crime), the post-amendment version of Section 230 allows private parties to bring civil actions and states to bring criminal charges arising out of conduct that they allege would constitute a federal crime.[109]

- The DMCA's safe harbors are also only available to tech companies that avoid so-called "red flag" knowledge of infringement. The DMCA provides that even in the absence of actual knowledge of infringement on their services, platforms may be liable if they are "aware of facts or circumstances from which infringing activity is apparent." 17 U.S.C. 512(c)(1)(A)(ii). Given the extensive content reviews companies engage in to prevent other forms of objectionable content, they must take expeditious action to remove content when red-flag knowledge does arise.

B - Discrimination Protections

- A line of cases starting with *Roommates.com* have held that when a service provider can be said to have "developed" content, in whole or in part, it may be liable under discrimination laws. Although this generally applies in contexts far removed from discrimination, it highlights that anti-discrimination laws are enforceable against tech platforms when they take an active role in facilitating the creation of the content in question.

A line of cases starting with Roommates.com have held that when a service provider can be said to have "developed" content, in whole or in part, it may be liable despite under discrimination laws.

  - *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (*en banc*). (online service provider violated Fair Housing Act and state nondiscrimination laws by requiring end users to create profiles indicating, among other things, preferences regarding sex, family status, and sexual orientation of potential roommates);

[107] 132 Stat. 1253 (Apr. 11, 2018).

[108] 18 U.S.C. §§ 1591(e)(4), 2421A(a).

[109] *See* 47 U.S.C. § 230(e)(5).

- *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1200 (10th Cir. 2009) (affirming liability where its business model revolved around its compensation of researchers for unlawfully obtaining and sharing sensitive private information);
- *Perkins v. Linkedin Corp.*, No. 13-cv-04303 (N.D. Cal. 2014) ($13 million settlement for violating the Electronic Communications Privacy Act and state laws by using LinkedIn members' names, photographs, and email contacts to grow its member base through a service called "Add Connections");
- *Fraley v. Facebook, Inc.*, 3:11-cv-01726 (N.D. Cal. 2013) ($20 million settlement for misappropriating Facebook users' names, profile photos, and likenesses in paid advertisements without consent);
- *Swift v. Zynga Game Network, Inc.*, No. C 09–05443 SBA, 2010 WL 4569889 (N.D. Cal. Nov. 3, 2010) (alleging state law violations for deceiving users by providing "special offer" transactions in connection with the company's free online video games).

C - Election Advertising

- The Federal Election Commission (FEC) and states have long regulated political ads.
  - States such as Washington,[110] Maryland,[111] and New York[112] have passed laws that regulate political ads on tech platforms. For example, Washington requires platforms that accept state and local political ads to keep detailed records about these ads and make information about them available to the public. New York requires platforms to verify advertiser registration with the New York State Board of Elections and create an online archive of political ads. State attorneys general have leveraged these laws to bring actions against large tech companies like Facebook and Google. For example, in December 2018, Facebook and Google agreed to pay over $400,000 to settle an action brought by the Washington attorney general for allegedly failing to maintain information for Washington state political ads placed on their platforms.[113]
  - Efforts are currently underway to expand the FEC's authority to, among other things, regulate the conduct of platforms that host political ad content. For example, the FEC recently opened a new rulemaking that would expand its authority to regulate disclaimers in online political ads.[114]

---

[110] RCW § 42.17A.

[111] MD SB875.

[112] N.Y. Elec. Law §§ 14-106 to 107.

[113] *State of Washington v. Facebook, Inc.*, No. 18-2-14129-0 (Wash. Sup. Ct. 2018); *State of Washington v. Google, Inc.*, No. 18-2-14130-3 (Wash. Sup. Ct. 2018).

[114] 83 Fed. Reg. 12864.

3 - BUSINESS CONDUCT

Essentially every aspect of a business's conduct undergoes scrutiny by a litany of federal and state laws that regulate its internal and external practices. The federal government uses antitrust laws to ensure that anticompetitive business conduct does not harm consumers. Tax laws regulate businesses' conduct according to government policy preferences (for example, tax breaks for employer health insurance benefits). Environmental laws regulate how businesses interact with the world at large. Tort and product-safety laws regulate how businesses interact with customers, other users of their products, and third parties. Labor and employment laws regulate how businesses interact with workers. Securities laws regulate how businesses interact with investors. Import/export laws regulate how businesses interact with foreign nations. In the same vein as all of the above, antitrust laws regulate how businesses interact with their competitors. Prominent examples of these laws are highlighted below:

A - Federal Antitrust

i - Agencies, statutes, and regulatory guidance

- The DOJ Antitrust Division and the FTC share federal antitrust authority: DOJ through the Sherman Antitrust Act[115] and other competition laws, which prohibit restraints of trade and monopolization; the FTC through the Federal Trade Commission Act,[116] which prohibits unfair methods of competition including violations of those same antitrust laws[117]; and both through the Clayton Act,[118] which prohibits mergers, acquisitions, and similar transactions that may substantially lessen competition or to tend to create a monopoly. In addition, under the Hart–Scott–Rodino Antitrust Improvements Act[119] and the agencies' Premerger Notification Program,[120] businesses and individuals must give notice to DOJ and the FTC, and observe a waiting period to permit investigation, before closing a merger or acquisition above a certain

[115] 15 U.S.C. §§ 1-7.

[116] 15 U.S.C. §§ 41-58.

[117] DOJ has exclusive authority over criminal enforcement of the antitrust laws but otherwise, due to the interpretation of the FTC Act by the FTC and the courts, the FTC's ability to enforce the antitrust laws is co-extensive with the DOJ's. In addition, the FTC can, and does, refer criminal matters to DOJ for prosecution.

[118] 15 U.S.C. §§ 12-18, 19-27.

[119] 15 U.S.C. § 18a.

[120] See the FTC's explanatory guide at https://www.ftc.gov/enforcement/premerger-notification-program.

value threshold.[121] As a result, the federal antitrust laws prohibit all types of conduct that could be characterized as anticompetitive, even in the attempt stage.[122]

ii - Cartel enforcement

- DOJ''s cartel enforcement applies to criminal conspiracies to fix prices, rig bigs, allocate customers or territories, or engage in similar "hard core" criminal anticompetitive conduct, and permits criminal sanctions including maximums of $1 million in fines and 10 years of prison time for individuals and, for corporations, a fine of up to $100 million[123] or twice the gross gain or loss (whichever is greater).[124] Both individuals and corporations may be subject to felony convictions and the consequences that follow, such as ongoing antitrust compliance monitoring and debarment from government contracts. Cases typically involve products because price comparison and price fixing is more feasible for products than for services; however, the anti-cartel laws apply equally to service industries.
    - *Electrolytic capacitors*[125] (conspiracy to fix prices and rig bids of certain electrolytic capacitors).
    - *Lithium Ion Battery Cells*[126] (conspiracy to fix prices of cylindrical lithium ion battery cells for use in notebook computer battery packs).
    - *Optical Disk Drives*[127] (conspiracy to rig optical disk drive procurement events).
    - *Cathode Ray Tubes*[128] (conspiracy to fix prices, reduce output, and allocate market shares for color display tubes).
    - *Liquid Crystal Display Panels*[129] (conspiracy to fix prices of thin-film transistor liquid crystal display panels for use in computer monitors and laptops).

---

[121] The FTC revises the thresholds annually to respond to changes in the economy. The lowest current threshold is $84.4 million; see the FTC's explanatory guide, *supra* note 126, and the list of current thresholds at https://www.ftc.gov/enforcement/premerger-notification-program/current-thresholds. Note that while deals below the lowest threshold are not subject to the waiting period, the agencies have authority to challenge such "nonreportable" deals, and frequently do. *See* Leslie Overton, Deputy Asst. Att'y Gen., U.S. Dept. of Justice, "Non-reportable Transactions and Antitrust Enforcement" (Apr. 25, 2014), https://www.justice.gov/atr/file/517791/download. In fact, "the agencies can challenge transactions, before or after consummation, regardless of whether the transaction is subject to HSR notification." *Id.*

[122] *See* FTC's Guide to Antitrust Laws, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws.

[123] 15 U.S.C. § 1.

[124] 18 U.S.C. § 3571(d).

[125] See, e.g., United States v. NEC Tokin Corp., 15-cr-00426 (N.D. Cal. 2015).

[126] See, e.g., United States v. Sanyo Electric Co., Ltd., 13-cr-00472 (N.D. Cal. 2013).

[127] See, e.g., United States v. Hitachi-LG Data Storage, Inc., 11-cr-00724 (N. D. Cal. 2011).

[128] See, e.g., United States v. Samsung SDI Company, Ltd. 11-cr-00162 (N.D. Cal. 2011).

[129] *See, e.g.*, *United States v. Sharp Corp.*, No. 08-cr-00802 (N.D. Cal. 2008).

- DOJ and the FTC maintain multiple policy statements and official guidelines as to antitrust enforcement -- see generally DOJ's Guidelines and Policy Statements web page[130] -- nearly all of which apply to the technology industry. Several of these specifically cover technology industries, including the Antitrust Policy Statement on Sharing of Cybersecurity Information.[131] These Guidelines and Policy Statements explain enforcement priorities and philosophies that effectively regulate technology companies by setting parameters developed by DOJ.

iii - Mergers and Acquisitions

- The agencies can challenge both proposed and consummated transactions that may reduce competition under Section 7 of the Clayton Act. In addition, under the HSR Act, the DOJ and FTC have an opportunity to review transactions above a certain size prior to consummation, which avoids the difficulty of unwinding a completed acquisition. The fact that a company being acquired has no revenue -- such as an upstart technology company -- would not by itself exempt the transaction from reporting requirements. The agencies also can, and often do, challenge "nonreportable" deals (those that are not required to be notified), and have investigated and successfully unwound consummated tech mergers.
    - *United States v. CenturyLink, Inc.*, No. 17-cv-02028 (D.D.C. Oct. 2, 2017) (acquisition of Level 3 likely would substantially lessen competition for fiber-based enterprise and wholesale telecommunications and Intercity Dark Fiber).
    - *In re Broadcom Ltd.*, Dkt. No. C-4622 (F.T.C. Jul. 3, 2017) (acquisition of Brocade may substantially lessen competition in the fibre channel switch market).
    - *United States v. Charter Comms., Inc.,* No. 16-cv-00759 (D.D.C. Apr. 25, 2016) (proposed combination of Charter, Time Warner Cable, and Bright House Networks would reduce competition for video programming distribution).
    - *In re Verisk Analytics, Inc.*, Dkt. No. 9363 (F.T.C. Dec. 16, 2014) (acquisition of EagleView would likely reduce competition and result in a virtual monopoly in the U.S. market for rooftop aerial measurement products used by the insurance industry to assess property claims).
    - *In re CoreLogic, Inc.*, Dkt. No. C-4458 (F.T.C. Mar. 24, 2014) (acquisition of DataQuick would substantially lessen competition in the market for the licensing of national assessor and recorder bulk data).
    - *In re Nielsen Holdings N.V. & Arbitron Inc.,* Dkt. No. C-4439 (F.T.C. Feb. 28, 2014) (acquisition of Arbitron may tend to create a monopoly in the market for national syndicated cross-platform audience measurement services).

---

[130] DOJ Antitrust Division Guidelines and Policy Statements, https://www.justice.gov/atr/guidelines-and-policy- statements-0.

[131] DOJ and FTC Antitrust Policy Statement on Sharing of Cybersecurity Information (Apr. 2014), https://www.justice.gov/sites/default/files/atr/legacy/2014/04/10/305027.pdf.

- *United States v. Bazaarvoice, Inc.*, No. 13-cv-00133 (N.D. Cal. Jan. 10, 2013) (acquisition of PowerReviews reduced competition in the market for purchase product ratings and reviews platforms used by retailers and manufacturers).
- *In re CoStar Group, Inc.,* Dkt. No. C-4368 (F.T.C. Apr. 26, 2012) (acquisition by CoStar would reduce competition in the markets for real estate listings databases and information services).
- *In re Western Digital Corp.* Dkt. No. C-4350 (F.T.C. Mar. 5, 2012) (acquisition of Hitachi Global Storage Technologies would likely harm competition in the market for desktop hard disk drives used in personal computers).
- *United States v. AT&T Inc.,* No. 11-cv-01560 (D.D.C. Aug. 31, 2011) (merger of AT&T and T-Mobile would lessen competition in the markets for mobile wireless telecommunications services).
- *United States v. Verifone Sys., Inc.,* No. 11-cv-00887 (May 12, 2011) (acquisition of Hypercom would substantially lessen and eliminate competition in the sale of countertop and multi-lane POS terminals).
- *United States v. Google Inc. & ITA Software, Inc.*, No. 11-cv-00688 (D.D.C. Apr. 8, 2011) (acquisition of ITA would harm competition in the market for comparative flight search services).
- *In re Dun & Bradstreet Corp.*, Dkt. No. 9342 (F.T.C. May 7, 2010) (acquisition of Quality Education Data eliminated competition in the market for K-12 educational marketing databases).
- *United States v. AT&T Inc.*, No. 09-cv-01932 (D.D.C. Oct. 13, 2009) (acquisition of Centennial would harm competition for mobile wireless telecommunications services);
- *In the Matter of CCC Holdings Inc*, et al.. Dkt. No. 9334 (F.T.C. Nov. 25, 2008); *FTC v. CCC Holdings Inc.,* No. 08-cv-02043 (D.D.C. 2009) (Mitchell International's acquisition of CCC Information Services harmed competition in the market for systems used to estimate the cost of automotive collision repairs).

iv - Joint conduct

- This category involves agreements between businesses or individuals, which are not criminal (see Cartel enforcement, above) but nonetheless violate civil competition laws.
  - David Drummond, Senior Vice President, Corporate Development and Chief Legal Officer at Google, *Ending our agreement with Yahoo!* (Nov. 5, 2008), https://publicpolicy.googleblog.com/2008/11/ending-our-agreement-with-yahoo.html (abandoning joint venture because "after four months of review, including discussions of various possible changes to the agreement, it's clear that government regulators and some advertisers continue to have concerns about the agreement").
  - *In re 1-800 Contacts, Inc.,* Dkt. No. 9372 (F.T.C. Aug. 8, 2016) (series of bilateral agreements between 1-800 Contacts and numerous online sellers of contact lenses limited competition in certain online search advertising auctions).

- *United States v. eBay, Inc.*, No. 12-cv-58690 (N.D. Cal. Nov. 16, 2012) (no-solicitation and no-hiring agreement between eBay and Intuit suppressed competition); see also United States v. Adobe Systems, Inc., et al., No. 10-cv-01629 (D.D.C. 2010) (similar agreements among Adobe, Apple, Google, Intel, Intuit, and Pixar).
- *United States v. Verizon Comms. Inc.,* et al., No. 12-cv-01354 (D.D.C. Aug. 16, 2012) (agreements between Verizon Wireless and cable companies to sell bundled offerings and to develop integrated technologies through a research and development joint venture unreasonably restrained competition for broadband, video, and wireless services).
- *United States v. Apple Inc.,* et al., No. 12-cv-02826 (S.D.N.Y. Apr. 11, 2012) (anticompetitive conspiracy with publishing companies to raise, fix, and stabilize retail e-book prices); *see also United States v. Apple, Inc.*, 791 F.3d 290 (2d Cir. 2015).
- *United States v. Comcast Corp.,* et al., No. 11-cv-00106 (D.D.C. Jan. 18, 2011) (joint venture between Comcast and GE would reduce competition for video programming distribution).

v - Single Firm Conduct

- This category, also called "monopolization" in the U.S., involves anticompetitive conduct undertaken by a firm unilaterally; examples including tying, bundling, and predatory pricing. The DC Circuit's decision in the *Microsoft* case listed below is one of the most influential modern single-firm conduct cases; in fact, it is often cited as the reference case for setting forth basic standards of single-firm conduct liability. The underlying law in this area - Section 2 of the Sherman Act - is highly flexible, and allows for enforcement against behavior that causes *any* type of competitive harm, including harm to innovation (as in *Microsoft*), quality, choice, or price. "Free" or zero-price digital goods are equally subject to enforcement: for example, the DOJ's case against Microsoft in the late 1990s restricted Microsoft's ability to block third parties from competing with its own (free) Internet Explorer browser. Other examples include:
  - *FTC v. Qualcomm Inc.*, No. 17-cv-00220 (N.D. Cal. Jan. 17, 2017) (unlawful maintenance of a monopoly in cellular baseband processors through alleged anticompetitive licensing practices involving standard essential patents); see *id.* ECF No. 1490 (opinion and order ruling for FTC).
  - *In re Motorola Mobility*, Dkt. No C-4410 (F.T.C. Jul. 24, 2013) (unfair methods of competition related to licensing standard essential patents for cellular, video codec, and wireless LAN standards).[132]
  - *In re Intel Corp.*, Dkt. No. 9341 (F.T.C. Dec. 16, 2009) (used dominant market position to maintain its monopoly in the markets for central processing units and to create a monopoly in the markets for graphics processing units).

[132] The FTC has a long history of enforcement involving patented technologies and standard setting. *See, e.g., In re Dell Computer Corp.*, Dkt. No. C-3658 (F.T.C. Nov. 2, 1995); *In re Unocal Corp*., Dkt. No. 9305 (F.T.C. Mar. 4, 2003).

- *In re Negotiated Data Solutions LLC,* Dkt. No. C-4234 (F.T.C. Jan. 23, 2008) (harmed competition by breaking a FRAND licensing commitment that its predecessor made to standard setting organization).
- *In re Rambus, Inc.*, Dkt. No. 9302 (F.T.C. Jun. 18, 2002) (harmed competition for dynamic random access memory technology through deceptive participation in standard setting organization).
- *United States v. Microsoft Corp.*, No. 98-cv-01232 (D.D.C. May 18, 1998) (series of anticompetitive activities to protect Microsoft's monopoly in the market for PC operating systems); *see also United States v. Microsoft Corp.*, 253 F.3d 34 (D.C. Cir. 2001).

- In addition, the Antitrust Guidelines for the Licensing of Intellectual Property are a non-judicial mechanism that DOJ has used to effectuate its policy preferences.[133]

B - State antitrust enforcement

Nearly all states, such as California,[134] have enacted their own versions of the federal Sherman Act, and most states have "little-FTC Acts" that parallel the federal FTC Act to more broadly prohibit unfair methods of competition.[135] State attorneys general enforce these acts and regularly highlight their enforcement efforts in technology industries.[136]

i - Cooperation with federal regulators

- States often work with DOJ and the FTC to bring antitrust actions. For example, in *United States v. Comcast Corp.*,[137] DOJ filed suit with four states (California, Florida, Missouri, and Texas) to permanently enjoin a proposed joint venture and related transactions between Comcast and GE.
- State attorneys general and the DOJ met in September 2018 to coordinate and potentially increase antitrust enforcement against tech companies: "[s]tate officials are raising risks for companies such as Facebook Inc., Twitter Inc., and Alphabet Inc.'s Google as the states begin piecing together a coordinated legal strategy for confronting the firms over alleged antitrust violations and data-privacy abuses."[138]

---

[133] DOJ and FTC Antitrust Guidelines for the Licensing of Intellectual Property (Jan. 2017), https://www.justice.gov/atr/IPguidelines/download.

[134] *See* California's Cartwright Act, Cal. Bus. & Prof. Code § 16720.

[135] *E.g.*, California's Unfair Practices Act, Cal. Bus. & Prof. Code § 17000 *et seq*., and Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*.

[136] *E.g.,* Antitrust Highlights, Office of the Attorney General of the State of California, https://oag.ca.gov/antitrust/highlights.

[137] No. 11-cv-00106 (D.D.C. Jan. 18, 2011).

[138] John D. McKinnon and Douglas MacMillan, "States Loom as a Regulatory Threat to Tech Giants," Wall Street Journal (Sept. 9, 2018), *available at* https://www.wsj.com/articles/states-loom-as-a-regulatory-threat-to-tech-giants-1536521239; *see also* Brian Fung and Tony Romm, "Inside the private Justice Department meeting that could lead to new investigations of Facebook,

ii - Follow-on enforcement

- In many cases, particularly after the DOJ announces charges or the resolution in a cartel case, State attorneys general file suits seeking damages for consumers in their respective jurisdictions. These suits can be filed in federal or state court.
    - *Florida v. Hitachi-LG Data Storage, Inc.*, No. 13-cv-01877 (N.D. Cal. Apr. 24, 2013) (optical disk drive manufacturers cartel follow-on litigation);
    - *California v. Samsung SDI Co., Ltd.*, et al, No. CGC-11-515784 (Sup. Ct. Cal. Nov. 8, 2011) (cathode ray tube manufacturers cartel follow-on litigation).

iii - Independent state actions

- State attorneys general also conduct investigations that have no federal origin, and which are increasingly focused on the tech industry. Recent examples include:
    - *New York Attorney General 2017 investigation of Compulink Technologies, Inc. & Milenio Technology, LLC* (obtaining injunctive relief after alleging Compulink, Milenio, and others engaged in bid-rigging in connection with bids submitted to New York State governmental entities for the deployment of digital communications cloud services).[139]
    - *Missouri Attorney General 2017 investigation of Google* (investigation, as part of AG's series of "Tech Investigations," into whether Google has violated state antitrust and consumer protection laws by taking improper steps to enhance its alleged power in search[140]).[141]
    - *New York Attorney General 2013 Seamless North America, LLC / GrubHub, Inc. merger review* (investigating the competitive implications of the proposed combination of food ordering platforms Seamless and GrubHub and forcing merging parties to ensure that tips are passed to employees as intended).[142]

C - Private antitrust litigation

- In addition to federal and state antitrust enforcement, injured companies or consumers can bring their own lawsuits to recover treble damages, supported by a highly active plaintiffs' bar.

Google and other tech giants," Washington Post (Sept. 25, 2018), https://www.washingtonpost.com/technology/2018/09/25/inside-big-meeting-federal-state-law-enforcement-that-signaled-new-willingness-investigate-tech-giants/.

[139] *In the Matter of the Investigation by Eric T. Schneiderman, New York AG, of Compulink Tech., Inc. and Milenio Tech., LLC*, Assurance No. 17-137 (July 2017).

[140] "AG Hawley Serves Additional Investigative Subpoena on Google," Office of the Missouri Attorney General, https://www.ago.mo.gov/home/breaking-news/ag-hawley-serves-additional-investigative-subpoena-on-google.

[141] "Tech Investigations," Office of the Missouri Attorney General, https://www.ago.mo.gov/home/working-for-you/ tech-investigations.

[142] Statement by the Office of the Attorney General of the State of New York as to the Proposed Combination of Seamless North America, LLC and GrubHub, Inc., https://ag.ny.gov/press-release/ag-schneiderman-announces-agreement-internet-food-delivery-company-grubhub.

The federal government sees such private plaintiffs as "private enforcers" who complement federal and state enforcement efforts.[143] Examples of private antitrust cases involving the technology services industry abound, including:

- *SC Innovations, Inc. v. Uber Technologies, Inc.,* No. 18-cv-07440 (N.D. Cal. filed 2018, litigation ongoing) (former Uber competitor alleging that Uber's predatory pricing and other anticompetitive tactics undermined competition and created a monopoly); *Malden Trans., Inc. v. Uber Technologies, Inc.*, No. 16-cv-12538 (D. Mass. filed 2016, trial scheduled July 2019) (Taxi companies brought consolidated action against ride-sharing service alleging attempt to monopolize); *see also Meyer v. Kalanick*, No. 15-cv-09796 (S.D.N.Y. filed 2015) (alleging that Uber's use of its pricing algorithm constitutes a price-fixing conspiracy), 868 F. 3d 66 (2d Cir. 2017) (mandating arbitration of the claims).
- *Dreamstime v. Google*, 3:18-cv-01910 (N.D. Cal) (alleging Google had maintained monopoly in image search advertising by "tanking" the search ranking of services that provided stock photos," dismissed 2019)
- *Location Svcs, LLC v. Digital Recognition Network, Inc.*, 18-cv-00744 (N.D. Tex., dismissed 2018) (alleging Digital Recognition violates federal and state antitrust and unfair competition laws by enforcing its one-year non-competition provision and by controlling prices on the sale of license plate recognition data).
- *Haier America Trading, LLC v. Samsung Elec., Co., Ltd.* et al., No. 17-cv-00921 (N.D.N.Y., dismissed 2018) (challenging patent licensing practices related to digital television technology).
- *EJ MGT LLC v. Zillow Group, Inc.,* No. 18-00584 (D.N.J., motion to dismiss pending) (alleging Zillow violated antitrust law by entering into agreements with partner brokers to display its "Zestimate" less prominently in their property listings)
- *Feitelson v. Google Inc.*, No. 14-cv-02007 (N.D. Cal. dismissed 2015) (alleging certain Google agreements restrict competition for general search and handheld search).
- *Social Ranger, LLC v. Facebook, Inc.*, No. 14-cv-01525 (D. Del. settled 2017) (alleging Facebook used its dominance in the social-game network market to anti-competitively obtain a monopoly in the virtual currency services market by requiring social-game developers to use Facebook Credits).
- *In re Graphics Processing Units (GPU) Antitrust Litig.*, No. M:07-cv-01826 (N.D. Cal.) (alleging defendants engaged in a conspiracy to fix the prices of GPUs.)[144]

---

[143] Note by the United States, Relationship Between Public and Private Antitrust Enforcement, Working Party No. 3 on Co-operation and Enforcement, OECD (June 15, 2015), https://www.ftc.gov/system/files/attachments/ us-submissions-oecd-other-international-competition-fora/publicprivate_united_states.pdf.

[144] The GPU case is particularly significant because the private plaintiffs continued their case even though the DOJ closed its investigation; thus, this is an example of private plaintiffs serving as a potential check on agency determinations. *See* Christine Caulfield, DOJ Ends GPU Antitrust Probe Against Nvidia, ATI, Law360, Oct. 13, 2008, https://www.law360.com/articles/72520/doj-ends-gpu-antitrust-probe-against-nvidia-ati; *see also In re Static Random Access*

- *In re Intel Corp. Microprocessor Antitrust Litig.*, No. 05-md-01717 (D. Del. class certification denied 2014) (alleging Intel unlawfully maintained microprocessor monopoly through exclusionary rebates).

D - Patents

i - Standard-setting and FRAND commitments

- Patent holders agree to substantial curtailment of their IP rights when their patents are incorporated into a standard. The rewards of having patented a technology are tempered by antitrust considerations.
- Patent holders often decide to contribute technology to a standard in return for limiting its return to a fair, reasonable and nondiscriminatory ("FRAND") royalty.
- Royalty rates are often calculated in infringement cases based on the "Georgia-Pacific" factors.[145]
  - However, the FTC's 2011 Report on the IP Marketplace recommended modifications to the Georgia-Pacific factors.[146]
  - Courts have adopted the FTC's recommendations.[147]
  - As a result, the methodology applied to determine what is a reasonable royalty rate considers four factors: (1) the economic value of the technology independent of the fact that it has been incorporated into the standard; (2) the importance to the product; (3) benchmarking against similar patents; and (4) the other royalties that the patent-implementer must pay.[148]

ii - Government and private enforcement

- The government has targeted technology companies in particular through litigation aimed at alleged violations of standard essential patent holders' FRAND commitments and licensing practices.
  - *FTC v. Qualcomm Inc.*, No. 17-cv-00220 (N.D. Cal. Jan. 17, 2017);

Memory (SRAM) Antitrust Litig., No. 07-md-01819 (N.D. Cal. filed 2007, settlement approved 2011 after DOJ closed its investigation in 2008).

[145] *Georgia-Pacific Corp. v. U.S. Plywood Corp.*, 318 F. Supp. 1116, 1120 (S.D.N.Y 1970), *modified and aff'd*, 446 F.2d 295 (2d Cir. 1971).

[146] FTC, The Evolving IP Marketplace: Aligning Patent Notice and Remedies with Competition ("2011 Report") at 184-185, https://www.ftc.gov/reports/evolving-ip-marketplace-aligning-patent-notice-remedies-competition.

[147] *See, e.g., In re Innovatio IP Ventures, LLC Patent Litig.*, 2013 WL 5593609 at *5-6 (N.D. Ill. Oct. 03, 2013); *Microsoft Corp. v. Motorola, Inc.*, 2013 WL 2111217 at *3, *12 (W.D.Wash. Apr. 25, 2013).

[148] *See* Jury Instructions and Verdict, *Realtek Semiconductor Corp. v. LSI Corp.*, Case No. C-12-3451-RMW (N.D. Cal. filed Feb. 23, 2014);

- *In re Motorola Mobility LLC*, No. C-4410 (F.T.C. July 23, 2013) (complaint).[149] Google, which by then owned Motorola Mobility, agreed to a consent order that limits its ability to seek injunctive relief and requires it to arbitrate disputes over FRAND licensing terms before it may seek an injunction;
- *In re Robert Bosch GmbH*, No. C-4377 (F.T.C. Apr. 24, 2013) (decision and order).[150] Bosch agreed to cease seeking injunctive relief and agreed to divest a business line.

E - General Corporate Law

Technology companies are also subject to the dictates of all the general corporate laws governing the sectors in which they operate, including:

i - Employment and non-discrimination

- Technology companies' innovative business models, such as "gig" work scheduled at the discretion of the worker, often make them susceptible to employment litigation.
  - *Zenelaj v. Handybook Inc.*, 82 F. Supp. 3d 968 (N.D. Cal. 2015) (compelling arbitration of claims that house-cleaning and home-repair platform was misclassifying gig workers as independent contractors);
  - *Otey v. CrowdFlower, Inc.*, 2014 WL 1477630 (N.D. Cal. 2014) (claims for wage-and-hours violations and misclassification settled for over half a million dollars);
  - *Singer v. Postmates Inc.*, No. 4:15-cv-01284 (N.D. Cal. 2015) (claims that delivery-service platform misclassified gig workers as independent contractors settled for $8.75 million);
  - *Levin v. Caviar, Inc.*, No. 3:15-cv-01286 (N.D. Cal. 2015) (claims that delivery-service platform misclassified gig workers as independent contractors settled after arbitration);
- Technology companies have also faced anti-discrimination suits.
  - *Damore, et al. v. Google, LLC*, No. 18CV321529, complaint (Cal. Super. Ct., Santa Clara Cty., Jan. 8, 2018) (allegations of discrimination based on political opinions survived motion to dismiss in June 2019 and litigation is ongoing);
  - *Beardsley v. Oracle Corp.*, No. 19-cv-02985 (D. Ariz. filed 2019) (alleging age and gender discrimination; court discouraged motions to dismiss and litigation is ongoing);
  - *Estle v. IBM Corp.*, No. 7:19-cv-02729 (S.D.N.Y. filed 2019) (alleging age discrimination in layoffs).

[149] In the Matter of Motorola Mobility, LLC and Google, Inc., No. C-4410 (July 2013).

[150] In the Matter of Bosch (Robert Bosch GmbH), No. C-4377 (April 24, 2013).

ii - Securities and financial regulation

- Technology companies are major targets for financial regulatory lawsuits because many are high-profile companies led by high-profile executives and are watched closely by stock market investors and the government.
    - *SEC v. Musk*, No. 18-cv-08865 (S.D.N.Y. filed 2018) (alleging and ultimately settling claim that Tesla CEO's Tweets misled investors); see also *In re Tesla, Inc. Securities Litig.*, No. 3:18-cv-04865-EMC (N.D. Cal.) (same);
    - *In re Alphabet Securities Litig.*, No. 18-cv-06245-JSW (N.D. Cal.) (alleging false statements regarding software glitches in Google+ social network, litigation ongoing);
    - *Lopes v. Fitbit, Inc.*, No. 3:18-cv-06665-JST (N.D. Cal.) (alleging false statements regarding financial projections, including based on CEO's comments during CNBC interview);
    - *Nemore v. Renovate America, Inc.*, No. BC701810 (Cal. Super. Ct., Los Angeles Cty., Jan. 24, 2019) (home-improvement financing platform alleged to have engaged in predatory lending, knowing that borrowers could not afford to repay loans for energy-efficiency home improvements known as Property Assessed Clean Energy (PACE) loans).

iii - Product liability and consumer safety

- Since technology companies typically specialize in producing innovative new products and services, there is inherently greater risk that consumers will not know how to use them appropriately, which often leads to tort litigation.
    - *McLellan et al v. Fitbit, Inc.*, No. 16-cv-00036 (N.D. Cal.) (allegations that products did not accurately monitor heart rate survived motion to dismiss; litigation is ongoing);
    - *Borgia v. Bird Rides Inc.*, No. 18-cv-09685 (C.D. Cal.) (alleging unsafe scooters, settlement negotiations ongoing);
    - *Huang v. Tesla Inc.*, No. 19CV346663 (Cal. Super. Ct., Santa Clara Cty, May 1, 2019) (wrongful death lawsuit brought by the estate of a driver who died after crashing allegedly due to Tesla's "Autopilot" feature).