Cahill

August 29, 2023

New FCC Task Force Seeks to Protect Consumer Privacy

Introduction

In 1973, a select committee of the United States Department of Health, Education & Welfare ("HEW") presented an exciting vision of the future: "[c]omputers linked together through high-speed telecommunications networks" of such power and speed as to finally slake humanity's age-old thirst for a universal system of recordkeeping.[1] But this promise was tempered by peril. As "the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused," HEW warned, "an individual's control over the personal information that he gives to an organization, or that an organization obtains about him" might slip.

Asserting that "personal privacy is essential to our well-being – physically, psychologically, socially, and morally" – HEW, balancing the rights and responsibilities of recorder and recorded, arrived at some basic principles for safeguarding it:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.[2]

Fifty years later, this formulation remains the cornerstone of the nation's privacy laws. But the threats that occasioned it remain as well, redoubling in complexity and severity with each leap forward in consumer communications. Rapid technological change has strained the ability of federal regulators to protect the vital right to privacy.

Jurisdictional turf wars among different federal regulators have further complicated the picture. As the Brookings Institution has observed, "the crazy quilt of federal privacy regulation that exists in America today" continues to grow, as identical services offered by ostensibly fungible communications providers "are subject to separate privacy regimes from multiple regulatory agencies," to the detriment of consumers and commerce alike.[3]

Shifting political winds have added to the challenges. In recent decades Congress and regulators alike have proposed and then abandoned certain privacy protections, only to embrace them again years later when political administrations and priorities shifted.

But sweeping change may be in the offing. On June 14, 2023, the Federal Communications Commission's ("FCC" or "Commission") announced the creation of a Privacy and Data Protection Task Force ("Task Force"). Charged with taking a whole-of-government approach and responsible for coordinating privacy and data protection

activities across the agency, the Task Force signifies a new commitment to ensuring "'cyber vigilance from every participant in our communications networks.'"[4]

The Origins of the FCC Privacy Regime

With the passage of the Telecommunications Act of 1996,[5] Congress established a new legal framework governing carrier use and disclosure of customer proprietary network information ("CPNI") and other customer information obtained by carriers while providing telecommunications services. That framework added Section 222 to the Communications Act of 1934, as amended (the "Communications Act").[6] Balancing both competitive and consumer privacy interests, Section 222 codified and extended existing FCC protections concerning legitimate customer expectations of confidentiality for their personal information in the hands of telecommunications carriers.

Section 222 imposes a duty upon common carriers "to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers"[7] and, "[e]xcept as required by law or with the approval of the customer," limits a carrier's ability to use customers' private information to its provision of telecommunications service or supporting services.[8]

In 2007, the FCC further bolstered its privacy rules by adopting additional safeguards to protect customer information against unauthorized access and disclosure, including a process for notifying law enforcement when data breaches occur.[9] In enacting these revisions, the Commission authorized companies to "use forms of self-monitoring" to comply with the "fundamental duty to remain vigilant in their protection of CPNI."[10] The Commission opined that its regulatory enforcement authority provided carriers with adequate incentive to safeguard against unlawful activity and protect consumers' private information.[11]

During the Obama administration, the FCC took a second look at this largely self-policing privacy regime. Closely examining the policies and practices of individual carriers, the Commission's investigations culminated in a series of increasingly expansive consent decrees that prescribed multi-year compliance plans and assessed large penalties.[12] Verizon, Verizon Wireless, AT&T Services Inc., and other carriers entered into settlements and paid fines, sometimes totaling many millions of dollars, for various failures to protect customers' private information.

Privacy Concerns Expand to Broadband

Alongside targeted oversight, the Commission also considered structural reforms. In *Connecting America: The National Broadband Plan*, released in March 2010, the Commission observed that consumers' "limited knowledge (if any) about how their personal data are collected and used" might give rise to concerns that would constitute "a barrier to the adoption and utilization of broadband."[13] With a lack of clarity surrounding the responsibilities of those who collect and use individual data, the FCC looked to adopt policies that reflected consumers' desire to protect their sensitive personal information. Six years later, the Commission undertook to do just that, with a rulemaking intended to "apply the traditional privacy requirements of the Communications Act to the most significant communications technology of today: broadband Internet access service (BIAS)."[14]

Having reclassified BIAS as a common carrier under Title II of the Communications Act in 2015's *Open Internet Order*,[15] the Commission sought to ensure that consumers are able to understand what data their broadband provider is collecting, what the provider does with that data, and whether consumers are protected against the unauthorized disclosure of their information.[16] The resulting privacy framework, adopted in October 2016, would have operationalized Section 222 to safeguard "transparency, choice, and data security" as well as "heightened protection for sensitive customer information, consistent with customer expectations."[17]

But the proposed privacy framework proved controversial. While advocacy groups hailed the draft rules as a vital bulwark against corporate intrusion into sensitive matters, other scholars and industry groups questioned the potential effect of the proposed rules on competition, consumer welfare, and technological innovation. One of the most pointed critics of the proposed rules was FCC Commissioner Ajit Pai,[18] who had long objected to the putatively extralegal bent of the FCC's expanded privacy enforcement efforts.[19]

With Commissioner Pai's elevation to Chairman by President Trump in January 2017, the political winds shifted once again. The FCC halted implementation of the adopted privacy regulations one day before they were scheduled to go into effect,[20] giving itself additional time to act upon eleven pending petitions for reconsideration of the *BIAS Order*. In February 2017, Senator Jeff Flake (R-AZ) introduced a joint resolution[21] nullifying the *BIAS Order* under the auspices of the Congressional Review Act ("CRA"),[22] which was signed into law on April 3, 2017.[23] Two months later, in accordance with the CRA,[24] the Commission issued an order dismissing as moot the petitions for reconsideration and clarifying that the pre-*BIAS Order* CPNI regulations remained in effect.[25]

Six months later, the *Restoring Internet Freedom Order* was released, reversing what the Commission now referred to as the "misguided and legally flawed" decision to classify BIAS as a common carrier under Title II of the Communications Act.[26] The FCC's foray into expanding its privacy regime to broadband providers was thus stifled by the Commission itself. Despite assurances from the nation's major BIAS providers that there was nothing to fear,[27] some members of the public expressed concerns about the Commission's decision.[28]

A Question of Jurisdiction

Complicating the question of the FCC's oversight of broadband providers and other emerging communications modalities is the role of the Federal Trade Commission ("FTC").[29] Under the Federal Trade Commission Act,[30] the FTC is "empowered and directed" to prevent corporations "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[31] This directive does, however, exclude from its scope "common carriers subject to the Acts to regulate commerce"[32] – a phrase interpreted to include the Communications Act.[33]

The Communications Act defines a "common carrier," in pertinent part, as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy. . . ."[34] The FCC's own "regulatory interpretation" of this enabling statute[35] casts a common carrier as "a person engaged in rendering communication service for hire to the public."[36] Under both definitions, Congress has afforded the FCC exclusive authority to regulate communications common carriers and to "prescribe such rules and regulations as may be necessary in the public interest."[37]

Yet, with respect to evolving communications technologies, this statutory line is not as clear cut as it appears. As the Ninth Circuit confirmed in *Federal Trade Commission* v. *AT&T Mobility LLC*, the common carrier exemption is "activity-based, meaning that a common carrier is exempt from FTC jurisdiction only with respect to its common-carrier activities," rather than "status-based, such that an entity engaged in common-carrier activities is entirely exempt from FTC jurisdiction."[38]

The FTC and the FCC attempted to address this regulatory overlap by entering into a Memorandum of Understanding in 2015. In that document, the parties, mindful of the need to "avoid duplicative, redundant, or inconsistent oversight" in matters of overlapping authority, promulgated broad jurisdictional divisions.[39]

Despite this agreement, concerns about competing regulatory jurisdictions and effectuating comprehensive oversight of increasingly complex technologies remain. As the FTC explained to the Senate Subcommittee on

Consumer Protection, Product Safety, Insurance, and Data Security in 2018, the distinction between common carrier activities and other activities is difficult to apply "in today's marketplace where the lines between telecommunications and other services are increasingly blurred."[40]

Privacy Concerns Expand to Foreign Entities

In May 2019, the Trump Administration promulgated Executive Order 13,873, which declared a national emergency as to "the security, integrity, and reliability of information and communications technology and services provided and used in the United States."[41] Ten months later, Congress passed the Secure and Trusted Communications Networks Act of 2019, which prohibits the use of "certain Federal subsidies" administered by the FCC for acquisition of "communications equipment or services posing national security risks" and "provide[s] for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risk."[42]

In accordance with these directives, and consistent with agency funding prohibitions set forth in the National Defense Authorization Act for Fiscal Year 2019,[43] in 2020 the FCC designated Huawei Technologies Company and ZTE Corporation as national security threats for purposes of universal service support funding.[44] The FCC also created a $1.6 billion "Secure and Trusted Communications Networks Reimbursement Program" to subsidize smaller carriers to remove and replace covered equipment" manufactured by these entities.[45]

During the first year of the Biden Administration, consumers continued to face significant threats to data integrity and consumer privacy, the most notable of which also involved foreign entities. In August 2021, for instance, T-Mobile disclosed a hack that had compromised "the first and last names, birth dates, Social Security numbers and driver's license information" of some 54 million customers.[46] The perpetrator was subsequently revealed to be an American expatriate living in Turkey, who effectuated the breach by "scanning T-Mobile's known internet addresses for weak spots using a simple tool available to the public."[47] Separately, two months later the Commission revoked China Telecom (Americas) Corporation's domestic and international operational authority under Section 214 of the Communications Act, based in part on the "significant national security and law enforcement risks" attendant in allowing a state-owned actor to collect personally identifiable information from U.S. citizens.[48]

Jurisdictional Disputes Remain Unresolved

Meanwhile, Congress sought to resolve the longstanding question of FCC-FTC jurisdiction over convergent technologies by giving the FTC jurisdiction over cybersecurity enforcement. The Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, introduced by Senator Roger Wicker (R-MS) in July 2021, would have removed the common carrier exemption in FTC enforcement actions regarding "unfair or deceptive acts or practices with respect to the privacy or security of covered data."[49] Likewise, the American Data Privacy Protection Act, introduced by Representative Frank Pallone (D-NJ) in December 2022, was intended to establish a comprehensive data privacy framework, based on the principle of express consent, under the exclusive jurisdiction of the FTC.[50] Neither of these proposals, however, was enacted into law.

A different approach to privacy regulation was advanced, to the surprise of some, by the FTC itself. In October 2021, the FTC published a report on the privacy practices of six major Internet Service Providers ("ISPs") and three associated advertising firms. ISPs, the study found, "collect significant amounts of consumer information from the range of products and services that they offer" through means both opaque and misleading to the consumer.[51] In her remarks on the report, FTC Chair Lina M. Khan expressed her belief "that the Federal Communications Commission has the clearest legal authority and expertise to fully oversee" the "commercial data

practices" of ISPs – authority she hoped would be leveraged to "once again put in place the nondiscrimination rules, privacy protections, and other basic requirements needed to create a healthier market."[52]

The FCC Responds

Under the current administration, the FCC has renewed its focus on consumer privacy. In October 2021, the Commission proposed augmenting its CPNI rules to combat subscriber identity module ("SIM") swapping – a scheme by which "a bad actor convinces a victim's wireless carrier to transfer the victim's service from the victim's cell phone to a cell phone in the bad actor's possession" – and "port-out fraud," a means of acquiring a victim's phone number by "open[ing] an account with a carrier other than the victim's current carrier."[53] These schemes, the FCC asserted, permit malicious parties "to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone," warranting augmentation of its rules.[54] In July 2023, after a period of inactivity, the Commission introduced an updated version of the regulations, which would "require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider" and "immediately notify customers whenever a SIM change or port-out request is made on customers' accounts . . . ."[55]

On July 19, 2022, Jessica Rosenworcel, who was designated FCC Chair by President Biden in October 2021, sent correspondence "to the top 15 mobile providers requesting information about their data retention and data privacy policies and general practices," including geolocation data sharing agreements.[56] The replies "revealed a huge variation within the industry's data retention and consumer privacy protocol," prompting some consumer advocates to demand consistent standards.[57]

In January 2023, the FCC promulgated a proposed rulemaking that would, for the first time since 2007, update and strengthen its CPNI data breach reporting rules.[58] According to Chairwoman Rosenworcel, consumers "deserve to be protected against the increase in frequency, sophistication, and scale of . . . data leaks, and the consequences that can last years after an exposure of personal information,"[59] though some common carriers have questioned whether the enhanced regulatory burdens these rules impose outweigh this goal.[60]

With reports of hackable smart garage door openers[61] and extortion and terror campaigns waged by international malefactors using indoor and outdoor online cameras,[62] the Commission also proposed a new U.S. Cyber Trust Mark ("USCTM") program for Internet-enabled devices. While device security and integrity are not new concepts, this is the first initiative explicitly based on the notion that "increased interconnection also brings increased security and privacy risks."[63] Under USCTM, participation in which is voluntary, corporations will place a logo on products meeting government-developed cybersecurity criteria, "such that consumers will know when devices meet widely accepted security standards."[64]

The New Task Force

By far the Commission's most expansive initiative has been the creation of the Task Force on June 14, 2023 – a wholly new approach that accounts for the centrality of connectivity to "'every aspect of modern civic and commercial life.'"[65] In remarks on its launch, Chairwoman Rosenworcel stated that the "clear communications privacy authority" afforded the Commission under the Communications Act might not be enough to address the multiplying, multivariate forces behind ever-more complex privacy challenges: "[R]ight now we need to use the law, evolve our policies, and approach consumer privacy and data security with new vigor."[66]

The Task Force, led by the Chief of the Commission's newly expanded Enforcement Bureau, does this by coordinating "rulemaking, enforcement, and public awareness" initiatives undertaken by various components of the FCC "in the privacy and data protection sectors, including data breaches (such as those involving telecommunications providers) and vulnerabilities involving third-party vendors that service regulated communications providers."[67] It is distinguished in its "whole-of-government and public-private approach" to cybersecurity – one that looks beyond the responsibilities of service providers to consider, per the FCC's wide-ranging "discovery and subpoena authorities," supply chain integrity and national security concerns.[68] Ultimately, the Task Force is a means"to increase consumer trust and confidence" to "ensure the benefits of this new digital world do more than just exceed its burdens" and "make communications private, safe, and secure" in a fast-changing world.[69]

A little more than two months after its creation, the Task Force is in full swing. On July 28, 2023, the FCC issued a $20 million Notice of Apparent Liability against Q Link Wireless LLC and Hello Mobile Telecom LLC for allegedly failing to comply with the Commission's CPNI rules.[70] Chairwoman Rosenworcel stated that the action demonstrates how the Task Force can "use the law to get results" by coordinating the efforts of "technical and legal experts from across the agency."[71]

Conclusion

As threats to privacy continue to mount, it appears the FCC, by and through the Task Force, is rising to meet them. From decades of fractured jurisdiction, outmoded statutes and rules, and changing political philosophies, an initiative has emerged promising consistent, comprehensive, and adaptive privacy oversight in the communications space. The wisdom of any particular regulatory action will, of course, have to be judged on its merits. But if companies are no longer whipsawed between different regulatory agencies and regulatory regimes, that will be a huge step forward. With the regulatory balkanization of years past no longer an option in "an era of always-on connectivity,"[72] it appears that HEW's half-century-old vision of universally robust and reliable privacy protections for consumers may finally come to pass.

* * *

If you have any questions about the issues addressed in this memorandum or if you would like a copy of any of the materials mentioned, please do not hesitate to call or email the author Chérie R. Kiser (Partner) at ckiser@cahill.com or 202.862.8950 or email publications@cahill.com. Matthew L. Conaty (Counsel) is also recognized for his contribution to this memorandum.

[1] The Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens*, v (July 1973), https://epic.org/wp-content/uploads/2021/11/1973-hew-report.pdf.

[2] *Id.* at 33, 40-41.

[3] The Brookings Institution (Dec. 16, 2021), https://www.brookings.edu/articles/broadband-privacy-belongs-with-the-ftc-not-the-fcc/.

[4] Federal Communications Commission, *Chairwoman Rosenworcel Launches New 'Privacy And Data Protection Task Force'* (June 14, 2023) ("*Data Protection Launch*"), https://docs.fcc.gov/public/attachments/DOC-394384A1.pdf.

[5] Pub. L. No. 104-104, 110 Stat. 56 (1996).

[6] 47 U.S.C. § 222.

[7] 47 U.S.C. § 222(a).

[8] 47 U.S.C. § 222(c)(1).

[9] 47 C.F.R. §§ 64.2010(a), 64.2011; *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 22 FCC Rcd 6927, ¶ 1 (2007).

[10] *Id.* ¶ 34.

[11] *Id.* ¶ 35. As set forth in Section 64.2009 of the Commission's Rules, 47 CFR § 64.2009, carriers may exercise considerable discretion in complying with broad standards in such areas as employee training, CPNI use logs, and annual compliance statements.

[12] *Cf.* Troutman Hamilton, "Testing the Privacy Waters: Does Recent FCC Privacy Enforcement Signal the Reclassification of Broadband Internet Service Providers as Common Carriers?" *JD Supra* (Jan. 26, 2015).

[13] Federal Communications Commission, *Connecting America: The Rural Broadband Plan*, 53 (Mar. 17, 2010) ("Once consumers have shared their data, they often have limited ability to see and influence what data about them has been aggregated or is being used. Further, it is difficult for consumers to regain control over data once they have been released and shared."), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[14] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 2500, ¶ 2 (2016) ("*BIAS NPRM*").

[15] *Protecting and Promoting the Open Internet*, 30 FCC Rcd 5601 (2015).

[16] *BIAS NPRM* ¶ 14. The FCC proposed a new category of "customer proprietary information" that encompassed both CPNI and PII, encompassing such categories as "biometric information," location tracking data, employment and financial information, "unique device identifiers . . . and information identifying personally owned property." *Id.* ¶ 62.

[17] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911, ¶ 5 (2016) ("*BIAS Order*").

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.

[18] *See, e.g.*, *BIAS NPRM*, Dissenting Statement of Commissioner Ajit Pai, 31 FCC Rcd at 2638 (arguing that in lieu of "respecting both common sense" and its duty to the public interest, the Commission "simply favor[ed] one set of corporate interests over another").

[19] *See, e.g., TerraCom / YourTel Order*, Dissenting Statement of Commissioner Ajit Pai ("[A]n agency cannot at once invent and enforce a legal obligation. Yet this is precisely what has happened here. In this case, there is no pre-existing legal obligation to protect personally identifiable information . . . or notify customers of a PII data breach to enforce."), https://docs.fcc.gov/public/attachments/FCC-14-173A4.pdf.

[20] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 32 FCC Rcd 1793 (2017). *Cf.* David Shepardson, "FCC chair to block stricter broadband data privacy rules," *Reuters* (Feb. 24, 2017) ("Ajit Pai, the FCC chairman appointed by President Donald Trump, believes all companies in the 'online space should be subject to the same rules, and the federal government should not favor one set of companies over another' . . . ."), https://www.reuters.com/article/us-usa-fcc-broadband/fcc-chair-to-block-stricter-broadband-data-privacy-rules-idUSKBN163222.

[21] Senator Flake characterized the *BIAS Order* as "'midnight regulation [that] does nothing to protect consumer privacy'" – an "'unnecessary'" and "'confusing'" rulemaking that "'adds yet another innovation-stifling regulation to the Internet.'" Jon Brodkin, "GOP senators' new bill would let ISPs sell your Web browsing data," *Ars Technica* (Mar. 8, 2017).

[22] 5 U.S.C §§ 801 *et seq.* The resolution, S.J. Res. 34, centered on the *BIAS Order* as published in the Federal Register on December 2, 2016, 81 Fed. Reg. 87274.

[23] *See* Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017). Mindful of sharply divided public opinion over this outcome, the FCC and FTC agency heads jointly authored an op-ed claiming that "Congress's decision didn't remove existing privacy protections; it simply cleared the way for us to work together to reinstate a rational and effective system for protecting consumer privacy." Ajit Pai & Maureen Ohlhausen "No, Republicans didn't just strip away your Internet privacy rights," *The Washington Post* (Apr. 4, 2017), https://www.washingtonpost.com/opinions/no-republicans-didnt-just-strip-away-your-internet-privacy-rights/2017/04/04/73e6d500-18ab-11e7-9887-1a5314b56a08_story.html.

[24] *See* 5 U.S.C. §§ 801(f) ("Any rule that takes effect and later is made of no force or effect by enactment of a joint resolution under section 802 shall be treated as though such rule had never taken effect"), 802(a) (defining form of effective joint resolution).

[25] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, 32 FCC Rcd 5442 (2017).

[26] 33 FCC Rcd 311, ¶ 2 (2018).

[27] *See, e.g.,* Jacob Kastrenakes, "Comcast, AT&T, and Verizon say you shouldn't worry about gutting of internet privacy rules," *The Verge* (Mar. 31, 2017), https://www.theverge.com/2017/3/31/15138094/comcast-att-fcc-internet-privacy-rules-response.

[28] *See, e.g.,* Duarte & Calabrese, *supra*; Public Knowledge, The FCC Should Continue Its Strong Role in Protecting Broadband Privacy (July 10, 2017), https://publicknowledge.org/the-fcc-should-continue-its-strong-role-in-protecting-broadband-privacy/.

[29] *Cf.* Theodore Bolema, *There is Nothing Anemic About the FTC's Consumer Protection Capabilities*, 15 Free State Foundation 2 (Jan. 7, 2020) (comparing FTC and FCC enforcement powers over harmful practices undertaken by BIAS providers), https://iseg.wichita.edu/publications/there-is-nothing-anemic-about-the-ftcs-consumer-protection-capabilities/.

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.

[30] 15 U.S.C. §§ 41, *et seq.*

[31] 15 U.S.C. § 45(a)(2).

[32] *Id*.

[33] 15 U.S.C. § 44.

[34] 47 U.S.C. § 153(11).

[35] *Cf. Eagleview Technologies, Inc. v. MDS Associates*, 190 F.3d 1195, 1197 (11th Cir. 1999).

[36] 47 CFR § 101.3. *Cf. Federal Trade Commission v. American eVoice, Ltd*., 242 F. Supp. 3d 1119, 1124 (D. Mont. 2017) (delineating regulatory filings typical of common carrier status).

[37] 47 U.S.C. § 201(b); *see also* 47 U.S.C. § 151 (giving the FCC jurisdiction over interstate and foreign commerce in wire and radio communication).

[38] 883 F.3d 848, 850 (9th Cir. 2018). In reaching this conclusion, the Ninth Circuit cited both its own precedent regarding interstate and communications common carriers as well as the Supreme Court's holding in *FCC v. Midwest Video Corp.*, 440 U.S. 689, 701 n.9 (1979), which established that [a] cable system may operate as a common carrier with respect to a portion of its service only." Both the FTC and the FCC have long argued for this interpretation of the common carrier exemption. *See* No. 15-16585, *Federal Trade Commission v. AT&T Mobility LLC*, Answering Brief of the Federal Trade Commission (9th Cir. Feb. 3, 2016), https://www.ftc.gov/system/files/documents/cases/160203attresponsebrief2_0.pdf; No. 15-16585, *Federal Trade Commission v. AT&T Mobility LLC*, Brief of the Federal Communications Commission as Amicus Curiae in Support of Plaintiff-Appellee (May 30, 2017), https://docs.fcc.gov/public/attachments/DOC-345126A1.pdf.

[39] *FCC-FTC Consumer Protection Memorandum of Understanding*, 1 (Nov. 2015), https://docs.fcc.gov/public/attachments/DOC-336405A1.pdf. In 2017, the parties also signed a Memorandum of Understanding – *Restoring Internet Freedom: FCC-FTC Memorandum of Understanding* (Dec. 14, 2017), https://www.ftc.gov/system/files/documents/cooperation_agreements/fcc_fcc_mou_internet_freedom_order_1214_final_0.pdf – to divide responsibilities for enforcement of the restored 2010 Transparency Rule, which requires BIAS providers to "publicly disclose accurate information regarding the network management practices, performance characteristics, and commercial terms of its broadband internet access services sufficient to enable consumers to make informed choices regarding the purchase and use of such services and entrepreneurs and other small businesses to develop, market, and maintain internet offerings." 47 CFR § 8.1(a).

[40] *Prepared Statement Of The Federal Trade Commission: Oversight Of The Federal Trade Commission Before The Committee On Commerce, Science, And Transportation, Subcommittee On Consumer Protection, Product Safety, Insurance, And Data Security, United States Senate*, 16 (Nov. 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1423835/p180101_commission_testimony_re_oversight_senate_11272018_0.pdf.

[41] Exec. Order No. 13,873, 84 Fed. Reg. 22689 (2019).

[42] Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609); *see Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 35 FCC Rcd 14284 (2020) (implementing legislation).

[43] Pub. L. No. 115-232, 132 Stat. 1636, § 889(a)-(b)(1), (f)(2)-(3) (2018).

[44] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, 35 FCC Rcd 6604 (2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, 35 FCC Rcd 6633 (2020); *see also*

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, 34 FCC Rcd 11423 (2019).

[45] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 35 FCC Rcd 14284, ¶ 1 (2020).

[46] Drew FitzGerald, "T-Mobile Says 6 Million More Customer Files Accessed in Data Breach," David Uberti, *The Wall Street Journal* (Aug. 20, 2021), https://www.wsj.com/articles/t-mobile-says-6-million-more-customer-files-accessed-in-data-breach-11629468163; David Uberti, "T-Mobile Faces Regulatory Scrutiny After Hack," *The Wall Street Journal* (Aug. 19, 2021), https://www.wsj.com/articles/t-mobile-faces-regulatory-scrutiny-after-hack-11629401366; Drew FitzGerald & Robert McMillan, "T-Mobile Says Hackers Stole Data on More Than 40 Million People," *The Wall Street Journal* (Aug. 18, 2021), https://www.wsj.com/articles/t-mobile-says-hackers-stole-details-on-more-than-40-million-people-11629285376.

[47] Drew FitzGerald & Robert McMillan, "T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'," *The Wall Street Journal* (Aug. 27, 2021), https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105.

[48] *China Telecom (Americas) Corporation*, 36 FCC Rcd 15966, ¶ 72 (2021); *see also China Telecom (Americas) Corporation*, 35 FCC Rcd 15006 (2020); Federal Communications Commission, *Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of The Secure Networks Act* (Sept. 20, 2022), https://docs.fcc.gov/public/attachments/DA-22-979A1.pdf; Federal Communications Commission, *FCC Initiates Proceeding to Revoke Authority of Telecom Carriers Controlled by Communist China After Their Failure to Address National Security Concerns* (Mar. 17, 2021) ("After issuing Show Cause Orders last year to three telecom companies with ties to the communist regime in China, the FCC determined today that those carriers' responses failed to address the serious national security threats posed by their continued operation in the U.S. By initiating revocation proceedings as a result of this determination, the FCC moves to the final step in a process that could prohibit these carriers from continued operation in the U.S."), https://docs.fcc.gov/public/attachments/DOC-370862A1.pdf; *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84, ¶¶ 3, 8 (rel. Nov. 25, 2022) ("*Protecting Against National Security Threats*").

[49] S. 2499, 117th Cong. § 401(3) (2021).

[50] H.R. 8152, 117th Cong. (2022).

[51] Federal Trade Commission Staff, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers,* iv (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[52] *Remarks of Chair Lina M. Khan Regarding the 6(b) Study on the Privacy Practices of Six Major Internet Service Providers; Commission File No. P195402*, 2 (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597790/20211021_isp_privacy_6b_statement_of_chair_khan_final.pdf.

[53] *Protecting Consumers from SIM Swap and Port-Out Fraud*, 36 FCC Rcd 14120, ¶ 2 (2021).

[54] *Id.*

[55] Federal Communications Commission, *FCC Privacy Task Force Announces Proposed Rules to Protect Consumers' Cell Phone Accounts*, 1 (July 11, 2023), https://docs.fcc.gov/public/attachments/DOC-395019A1.pdf.

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.

[56] Federal Communications Commission, *Chairwoman Rosenworcel Probes Top Mobile Carriers on Data Privacy Practices* (July 19, 2022), https://docs.fcc.gov/public/attachments/DOC-385446A1.pdf.

[57] Keith Lewis, "Privacy advocates demand rules for mobile providers on data use," *Roll Call* (Sept. 6, 2022), https://rollcall.com/2022/09/06/privacy-advocates-demand-rules-for-mobile-providers-on-data-use/.

[58] WC Docket No. 22-21, *Data Breach Reporting Requirements*, Notice of Proposed Rulemaking, FCC 22-102, ¶ 10 (rel. Jan. 6, 2023), https://docs.fcc.gov/public/attachments/FCC-22-102A1.pdf.

[59] Federal Communications Commission, *Chairwoman Rosenworcel Circulates New Data Breach Reporting Requirements* (Jan. 12, 2022), https://docs.fcc.gov/public/attachments/DOC-379162A1.pdf.

[60] *See, e.g.,* Cynthia Brumfield, "Battle could be brewing over new FCC data breach reporting rules," *CSO* (Apr. 11, 2023), https://www.csoonline.com/article/574979/battle-could-be-brewing-over-new-fcc-data-breach-reporting-rules.html.

[61] *See, e.g.,* Joseph Cox, "Hackers Can Remotely Open Smart Garage Doors Across the World," *Vice* (Apr. 4, 2023), https://www.vice.com/en/article/pkadqy/hackers-can-remotely-open-smart-garage-doors-across-the-world-simpaltek.

[62] *See, e.g.,* Joseph Cox & Jason Koebler, "Ransomware Group Claims Hack of Amazon's Ring," *Vice* (Mar. 13, 2023), https://www.vice.com/en/article/qjvd9q/ransomware-group-claims-hack-of-amazons-ring.

[63] Federal Communications Commission, *Chairwoman Rosenworcel Announces Cybersecurity Labeling Program for Smart Devices*, 1 (July 18, 2023, https://www.fcc.gov/document/rosenworcel-announces-cybersecurity-labeling-program-smart-devices.

[64] *Id.* at 1.

[65] *Data Protection Launch*.

[66] *Remarks of FCC Chairwoman Jessica Rosenworcel to the Center for Democracy And Technology Forum On Data Privacy*, 2-3 (June 14, 2023) ("*CDT Remarks*"), https://docs.fcc.gov/public/attachments/DOC-394386A1.pdf.

[67] Federal Communications Commission, Privacy and Data Protection Task Force (July 11, 2023), https://www.fcc.gov/privacy-and-data-protection-task-force.

[68] *Id*.

[69] *CDT Remarks* at 4.

[70] *Q Link Wireless LLC and Hello Mobile Telecom LLC*, Notice of Apparent Liability for Forfeiture, FCC 23-59, ¶ 4 (rel. July 28, 2023).

[71] Federal Communications Commission, *FCC Proposes $20 Million Penalty Against Q Link and Hello Mobile for Apparently Failing to Protect Customer Data*, 1 (July 28, 2023) ("'With this enforcement action, all telecommunications service providers are on notice that protecting customers' data should be their highest priority, and we will use our authorities to ensure that they comply with their obligations to do so.'"), https://docs.fcc.gov/public/attachments/DOC-395581A1.pdf.

[72] *Data Protection Launch.*

This memorandum is for general information purposes only and is not intended to advertise our services, solicit clients or represent our legal advice.