epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 17, 2024

Loyaan A. Egal
Bureau Chief
Enforcement Bureau
Federal Communications Commission
45 L St NE
Washington, DC 20554

Dear Bureau Chief Egal,

We, the Electronic Privacy Information Center (EPIC), write to express our continuing support of the work by the Federal Communications Commission (FCC)'s Personal Data Protection Task Force and Enforcement Bureau to protect the privacy and personal data of consumers. This includes actions against voice carriers who know or should have known they were transmitting illegal calls[1] and greater accountability for service providers who fail to safeguard subscriber data.[2]

In order to be successful in advancing the FCC's mission, we urge the Task Force and Enforcement Bureau to emphasize six key privacy, cybersecurity, and consumer protection priorities, which we believe should be at the core of the Task Force's and Bureau's work moving forward. We also believe that the Commission should make greater use of several key enforcement authorities that advance those priorities.

I. Privacy, Cybersecurity, and Consumer Protection Priorities

1. SMS security: The Task Force and Bureau should audit the security of SMS messaging, including conducting assessments for potential network-level vulnerabilities and investigating instances of SIM swap/port-out fraud.

The FCC should take additional actions to fix the vulnerabilities in SMS and to ensure that our text messaging systems are not able to be misused to steal subscriber information and engage in identity theft. The Cybersecurity and Infrastructure Security Agency (CISA) has noted that SIM swapping is a favored tactic of cybercriminal groups such as Lapsus$, and has urged that the FCC and Federal Trade Commission (FTC) "incentivize better security at telecommunications providers by enacting penalties for fraudulent SIM swaps or lax controls."[3] Senator Ron Wyden has pushed for CISA to publish its 2022 unclassified report on SMS vulnerabilities such as those in the SS7 and Diameter protocols.[4] The Bureau and/or Task Force should investigate these vulnerabilities and should publish the contents of CISA's report, ideally in full but in summary if that is the only option.

2. **<u>Personal safety</u>: The Task Force and Bureau should investigate and report on the personal safety considerations of connected devices. These issues are well within the Commission's purview, as cybersecurity implicates personal safety, national security, and privacy.**

The FCC has a mandate to "promot[e] safety of life and property through the use of wire and radio communications."[5] This applies in particular to tech-facilitated abuse and stalking due to exploits in connected devices and communications infrastructure, as Congress articulated in the Safe Connections Act.[6] The Commission has explicit authority to investigate and publish reports related to this mandate, and it should do so.[7]

3. **<u>Data brokers</u>: The Task Force and Bureau should investigate, expose, and where appropriate take enforcement action against the commercial sale of Americans' data, including but not limited to indirect sales to foreign adversaries.**

Over the last decade we have seen a rapid expansion of data brokers engaged in the collection, sale, and transfer of sensitive personal data about communications subscribers. Both Congress[8] and the White House[9] have flagged specific concerns with the actions of data brokers controlled by foreign adversaries. But the FCC should play an active role in protecting subscribers against the misuse of their data, and the FCC should emphasize that foreign-originating or -based technologies[10] are not the only threat to Americans' privacy, data security, and national security.

Indeed, many data brokers are selling or providing access to sensitive subscriber data to a wide range of entities in ways that make that data readily available to foreign adversaries and criminals alike.[11] The FCC has relevant privacy authorities over carriers,[12] as well as providers of cable[13] and satellite,[14] and broadband internet.[15] The FCC should identify, expose, and where appropriate take enforcement action against harmful data broker practices. Chair Rosenworcel has already signaled the Commission's interest in this issue in the context of location data,[16] but the Bureau and Task Force should address the full ecosystem of harmful data broker practices that intersect with the FCC's jurisdiction. We note that with the sole exception of when carriers first began reporting on litigation against data brokers as part of their annual Customer Proprietary Network Information (CPNI) filings in 2008,[17] the four (now three) largest telecom companies have not reported a single legal action taken against any data broker in those annual filings.[18]

4. **<u>Location data</u>: The Task Force and Bureau should investigate potential misuses of subscriber location data and bring enforcement actions as appropriate. Chairwoman Rosenworcel's efforts to uncover more information about how carriers and their MVNOs operate were encouraging but warrant further action.**

As noted above, Chair Rosenworcel has taken encouraging steps to identify and expose how consumer location data is being collected and disclosed by carriers and their MVNOs.[19] However, more action is needed.[20] We urge the Bureau and Task Force to raise the visibility of how consumer location data is being used and to deter misuse through enforcement actions.[21]

5. **<u>IoT privacy and cybersecurity</u>: The U.S. Cyber Trust Mark (Trust Mark) is being rushed to implementation. The Task Force should urge the Public Safety and Homeland Security Bureau and the Lead Administrator to address privacy and security concerns, as otherwise the Trust Mark program may fail to achieve its core objective of strengthening consumer trust.**

We recognize that rollout of the Trust Mark is a priority for the Administration. But EPIC and peer organizations have emphasized that, at a minimum, sensor data must be included in the label if it is to meaningfully inform consumers about the risks posed by the devices in their homes, in their cars, and on their persons.[22] This is especially important in light of how these devices can and have been misused by abusers and stalkers.[23] Additionally, we again urge the Bureau and Task Force to use the Commission's investigatory authority to research and disclose threats to personal safety as they relate to these devices.[24]

6. **<u>Liability for deficient vendors</u>: There are too many breaches of subscriber data, and furthermore too many of these are the result of third-party systems or vendors used by carriers. The Task Force and Bureau should hold companies accountable for their failure to adequately vet their vendors.**

As we discuss further below, we urge the Bureau and Task Force to hold carriers responsible for activity that they know or should have known was being committed using their networks. This includes deficient cybersecurity practices by the vendors[25] those carriers have chosen to serve as custodians of their customers' data, including social security numbers.[26] EPIC recently supported the Commission's efforts to protect subscriber data in its Data Breach Reporting Requirements Rule;[27] we believe the FCC needs to continue to vigorously defend the breadth of its authority in this area.

II. <u>Underused Authorities</u>

We also recommend that the Task Force and Bureau make greater use of the agency's existing authorities—including but not limited to its powers under Sections 201(b), 217, and 154(n)—to achieve these ends.

Under **Section 201(b)**, the Commission may prohibit practices as unjust or unreasonable. The agency has cited to this authority in numerous enforcement actions and rules,[28] as well as in defense of its rules,[29] but the FCC has also neglected to invoke this provision in some instances in which it has applied.[30] The Supreme Court has said unambiguously that the FCC's authority under 201(b) is express and far-reaching, including "broad power to enforce all provisions of the statute."[31] We urge the Commission to be more aggressive in reminding regulated entities that it has this authority and that that the FCC (in partnership with the FTC)[32] will use that power to protect consumer interests like privacy.[33]

The Commission has already established that consumers have a reasonable expectation that their private or sensitive information will be protected by the carriers' obligations under Section 222.[34] The Commission should be doing more to leverage 201(b) to hold carriers accountable for failing to protect the privacy and security of consumer data. In particular, the FCC should follow the blueprint of the FTC in holding companies liable for the consumer harms they facilitate, including using means-and-instrumentalities liability to deter otherwise complicit providers.[35]

Under **Section 217**, the Commission may hold a carrier liable for the acts of its agent or other person acting on their behalf. Notably, "person" here includes individuals, partnerships, associations, joint-stock companies, trusts, and corporations. This could be a powerful tool for curtailing privacy violations and/or deficient cybersecurity practices of a carrier's vendors, as the Bureau has recently done,[36] as well as for holding carriers responsible for activity that they know or should have known is being committed using their networks. This is true even if the carrier operated through independent contractors.[37] In the context of the TCPA, multiple federal courts have considered how 47 U.S.C. § 217 can be used to hold officers personally liable,[38] and a similar analysis would apply to agents. The Commission has additionally invoked Section 217 in with respect to SIM swaps,[39] safely disposing of data about survivors of domestic violence,[40] and other contexts.[41] In at least one instance, civil society groups have encouraged the Commission to invoke 217 where a person acting on behalf of an internet service provider (ISP) impacts a subscriber's ability to choose an ISP.[42]

Under **Section 154(n)**, the Commission may investigate and study "all phases of the problem" of getting maximum effectiveness from the use of radio and wire communications in connection with safety of life and property. The Commission has taken numerous steps in its recent rulemakings that implicate the physical safety of individuals, whether that's 911 callers,[43] 988 callers,[44] or protections for survivors of domestic violence.[45] The FCC cannot allow a repeat of its disappointing investigation of breached subscriber location data, for example by failing to issue subpoenas to Securus[46] and failing to push back on overbroad assertions of confidential treatment.[47] With a few exceptions,[48] the agency seems to have relied primarily on the notice and comment process rather than conducting its own investigations to understand the equities at stake. We urge the Task Force and the Bureau to investigate these matters more fully, to ensure that its decisions are doing more good than harm, particularly where vulnerable or otherwise marginalized individuals are at enhanced risk.[49]

III. Conclusion

We thank you for the Task Force's and Bureau's efforts better safeguard consumer data held by communications companies, and we offer the above recommendations to carry forward that work. We urge you to focus especially on SMS security, personal safety, data brokers, location data, IoT privacy and cybersecurity, and liability for deficient vendors. If you have any questions or would like to discuss these matters further, please contact EPIC Counsel Chris Frascella at frascella@epic.org.

Respectfully submitted,

/s/ *Alan Butler*	/s/ *John Davisson*	/s/ *Chris Frascella*
Alan Butler	John Davisson	Chris Frascella
Executive Director	Director of Litigation	Counsel

Cc: Jane van Benten, Deputy Division Chief, Unwanted Communications
Edyael Casaperalta, Legal Advisor for Wireless, Public Safety and Consumer Protection, Office of Commissioner Gomez
Adam Cassady, Media and Wireline Advisor, Office of Commissioner Simington
Jeff Gary, Acting Assistant Division Chief, Privacy, Unfair/Deceptive Practices
Peter Hyun, Chief of Staff, Office of the Bureau Chief, Enforcement Bureau
Melissa Kirkel, Deputy Division Chief, Competition Policy Division, Wireline Competition Bureau
Douglas Klein, Assistant General Counsel, Office of General Counsel
Hannah Lepow, Legal Advisor for Media and Consumer Protection, Office of Commissioner Starks
Austin Randazzo, Associate Chief, Public Safety and Homeland Security Bureau, Office of the Bureau Chief
Victoria Randazzo, Legal Advisor, Office of the Bureau Chief, Enforcement Bureau
Philip Rosario, Deputy Bureau Chief, Office of the Bureau Chief, Enforcement Bureau
Carmen Scurato, Legal Advisor, Consumer and Public Safety, Office of Chairwoman Rosenworcel
Michael Snyder, Deputy Chief, Consumer and Government Affairs Bureau, Web & Print Publishing Division
Daniel Stepanicich, Assistant Division Chief, Unwanted Communications
Kristi Thompson, Division Chief, Telecommunications Consumers Division
Greg Watson, Chief of Staff, Office of Commissioner Carr

Endnotes

[1] *See, e.g.*, Robocaller Facilitators Must Cease and Desist, https://www.fcc.gov/robocall-facilitators-must-cease-and-desist.

[2] *See, e.g.*, T-Mobile Required to Change Business Practices After Data Breaches (Rel. Sept. 30, 2024), https://www.fcc.gov/document/t-mobile-required-change-business-practices-after-data-breaches [hereinafter "2024 T-Mobile Settlement"]; FCC Settles with AT&T for Vendor Cloud Breach (Rel. Sept. 17, 2024), https://www.fcc.gov/document/fcc-settles-att-vendor-cloud-breach [hereinafter "2024 AT&T Vendor Breach Settlement"]; TracFone to Pay $16M to Settle Data & Cybersecurity Investigation (Rel. July 22, 2024), https://www.fcc.gov/document/tracfone-pay-16m-settle-data-cybersecurity-investigation [hereinafter "2024 TracFone Settlement"]. *See also in re Data Breach Reporting Requirements*, Report and Order, WC Dkt. No. 22-21, FCC 23-111 at 96, Statement of Chairwoman Jessica Rosenworcel (Rel. Dec. 21, 2023), https://www.fcc.gov/document/fcc-adopts-updated-data-breach-notification-rules-protect-consumers-0 (noting Task Force's input) [hereinafter "2023 Data Breach Reporting Order"].

[3] Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus$ and Related Threat Groups* 37 (July 24, 2023), https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf. *See also* Comment of Electronic Privacy Information Center (EPIC), *in re Protecting Consumers from SIM-Swap and Port-Out Fraud*, WC Dkt. No. 21-341 (Jan. 16. 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1011728090306; EPIC and NCL Urge Ninth Circuit to Hold Telecoms Accountable for Weak Security Allowing SIM Swap Fraud (Aug. 7, 2023), https://epic.org/epic-and-ncl-urge-ninth-circuit-to-hold-telecoms-accountable-for-weak-security-allowing-sim-swap-fraud/.

[4] *See, e.g.*, Public Safety and Homeland Security Bureau (PSHSB) Requests Comment on Implementation of Measures to Prevent Location Tracking via The Diameter and Signaling System 7 Security Protocols, Request for Comment, PS Dkt. No. 18-99 at 4 n. 21 (Rel. Mar. 27, 2024), https://docs.fcc.gov/public/attachments/DA-24-308A1.pdf (citing to Letter from Ron Wyden, U.S. Senator, to Joseph Biden, President of the United States (Feb. 29, 2024),

https://www.wyden.senate.gov/imo/media/doc/wyden-phone-hacking-letter-to-president-biden.pdf). *See also* Reply Comment of EPIC, PS Dkt. No. 18-99 (May 28, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1052800568030; Fact Sheet, Cybersecurity Risks Caused by SMS Vulnerabilities, https://epic.org/documents/cybersecurity-risks-caused-by-sms-vulnerabilities/; EPIC Testifies at House Hearing on Securing Communications Networks (Jan. 10, 2024), https://epic.org/epic-testifies-at-house-hearing-on-securing-communications-networks/. By some estimates, there are more than 2.5 million tracking attempts using SS7 every year. *See, e.g.*, @Veritasium, *Exposing The Flaw in Our Phone System* at 25:10 (Sept. 21, 2024), https://www.youtube.com/watch?v=wVyu7NB7W6Y&t=1509s.

[5] 47 U.S.C. § 151.

[6] *See, e.g.*, *In re Supporting Survivors of Domestic and Sexual Violence*, Further Notice of Proposed Rulemaking, WC Docket No. 22-238 at ¶ 4 (Apr. 23, 2024), https://docs.fcc.gov/public/attachments/FCC-24-38A1.pdf [hereinafter "Safe Connections FNPRM"] (citing to Congress's explicit findings in the Safe Connections Act, including that "perpetrators of

violence and abuse . . . increasingly use technological and communications tools to exercise control over, monitor, and abuse their victims," and that "[c]ommunications law can play a public interest role in the promotion of safety, life, and property."); Comment of Consumer Reports, Carnegie Mellon University, Public Knowledge, EPIC, New York University, *in re Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 4-5 (Aug. 19, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10819759410275 [hereinafter "CMU CR et al IoT Comment"]; Comment of EPIC and Public Knowledge, *in re Supporting Survivors of Domestic and Sexual Violence*, WC 22-238 at 11 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105242630421222 [hereinafter "EPIC PK Connected Car Comment"].

[7] *See, e.g.*, EPIC PK Connected Car Comment at 25-26 (citing to 47 U.S.C. § 154(n)); Reply Comment of EPIC, *in re Cybersecurity Labeling for Internet of Things*, PS 23-239 at 6 (May 24, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1052456289771 [hereinafter "EPIC IoT FNPRM Reply Comment"]. The Federal Trade Commission (FTC) has taken a similar approach in publishing its 6(b) studies on internet service providers (ISPs) and on streaming services. *See generally* Fed. Trade Comm'n, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* (2021), *available at* 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; Fed. Trade Comm'n, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

[8] *See, e.g.*, Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes, H.R. 815, 118th Cong., https://www.congress.gov/bill/118th-congress/house-bill/815 (Division I prohibiting data brokers from selling data on Americans directly to countries of concern, Division H prohibiting various forms of support for applications controlled by foreign adversaries).

[9] *See* Statements and Releases, Fact Sheet: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data, White House Briefing Room (Feb. 28, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

[10] *See, e.g.*, Secure and Trusted Communications Networks Reimbursement Program, https://www.fcc.gov/supplychain/reimbursement; *In re China Telecom (Americas) Corporation*, Order on Revocation and Termination, GN Dkt. No. 20-109 (Rel. Nov. 2, 2021), https://docs.fcc.gov/public/attachments/FCC-21-114A1.pdf; *In re Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, Order and Notice of Proposed Rulemaking, IB Dkt. No. 23-119, MD Dkt. No. 23-134 (Rel. Apr. 25, 2023), https://docs.fcc.gov/public/attachments/FCC-23-28A1.pdf; *In re Cybersecurity Labeling for Internet of Things*, Report and Order and Further Notice of Proposed Rulemaking, PS Dkt. No. 23-239, FCC 24-26 (Rel. Mar. 15, 2024), https://www.fcc.gov/document/fcc-adopts-rules-iot-cybersecurity-labeling-program.

[11] *See, e.g.*, Press Release, Wyden Statement on Data Export Executive Order (Feb. 28, 2024), https://www.wyden.senate.gov/news/press-releases/wyden-statement-on-data-export-executive-order; Justin Sherman, *Data Brokerage and Threats to U.S. Privacy and Security*, Written Testimony to U.S. Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector" (Dec. 7, 2021), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf; EPIC IoT FNPRM Reply Comment at 1 ("Requiring disclosure of all data transfers to high-risk countries, including indirect transfers, is easily administrable.").

[12] *See, e.g.*, 47 U.S.C. § 201(b); 47 U.S.C. § 222.

[13] *See, e.g.*, 47 U.S.C. § 551. *See also* Cox Communications to Pay $595,000 to Settle Data Breach Investigation, EB-IHD-14-00017829, DA 15-1241 (Rel. Nov. 5, 2015), https://www.fcc.gov/document/cox-communications-pay-595000-settle-data-breach-investigation [hereinafter "Cox Order"].

[14] *See, e.g.*, 47 U.S.C. § 338(i).

[15] *See, e.g.*, *In re Safeguarding and Securing the Open Internet, Restoring Internet Freedom*, Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, WC Dkt. Nos. 23-320, 17-108 (Rel. May 7, 2024), https://docs.fcc.gov/public/attachments/FCC-24-52A1.pdf [hereinafter "2024 Title II Order"], *but see* Order to Stay Pending Review, *In re: MCP No. 185 Open Internet Rule (FCC 24-52)* No. 24-7000 (6th Cir. Aug. 1, 2024).

[16] *See, e.g.*, Rosenworcel Probes Mobile Carriers on Data Privacy Practices (Rel. July 19, 2022), https://www.fcc.gov/document/rosenworcel-probes-mobile-carriers-data-privacy-practices; Rosenworcel Shares Mobile Carrier Responses to Data Privacy Probe (Re. Aug. 25, 2022), https://www.fcc.gov/document/rosenworcel-shares-mobile-carrier-responses-data-privacy-probe [hereinafter "Rosenworcel Shares Responses"]; Chairwoman on Safe Connected Cars for Domestic Violence Survivors (Rel. Jan. 11, 2024), https://www.fcc.gov/document/chairwoman-safe-connected-cars-domestic-violence-survivors.

[17] *See, e.g.*, Statement of Verizon, *in re Annual CPNI Certification*, EB Dkt. No. 06-36 (Mar. 3, 2008), https://www.fcc.gov/ecfs/search/search-filings/filing/5515012723;

Statement of Sprint Nextel Corp., *in re Annual CPNI Compliance Certification*, EB Dkt. No. 06-36 (Mar. 3, 2008), https://www.fcc.gov/ecfs/search/search-filings/filing/5515012959.

[18] Per annual filings in EB Dkt. No. 06-36 as of March 1, 2024. *See also* FCC Enforcement Advisory No. 2024-01, DA 24-125, *Telecommunications Carriers and Interconnected VoIP Providers Must File Annual Reports Certifying Compliance with Commission Rules Protecting Customer Proprietary Network Information*, EB Dkt. No. 06-36 at 4, 5, 7, 8 (Rel. Feb. 9, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10209181854750 (noting annual requirement to report on any actions taken against data brokers).

[19] *See supra* note 16.

[20] *See* Rosenworcel Shares Responses, *supra* note 16 ("Additionally, I have asked the Enforcement Bureau to launch a new investigation into mobile carriers' compliance with FCC rules that require carriers to fully disclose to consumers how they are using and sharing geolocation data"). There has been no public update since August 25, 2022.

[21] *See, e.g.*, FCC Fines Largest Wireless Carriers for Sharing Location Data (Rel. Apr. 29, 2024), https://www.fcc.gov/document/fcc-fines-largest-wireless-carriers-sharing-location-data; 2024 Title II Order at ¶¶ 350-51.

[22] *See, e.g.*, Reply Comment of EPIC, Clinic to End Tech Abuse (CETA), Madison Tech Clinic, Public Knowledge, and Ranking Digital Rights, filed by the Communications and Technology Law Clinic (IPR) at Georgetown Law, *in re Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 17, 21, 23-26 (Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111054758013 (citing to CMU label model, describing IoT as vector for intimate partner violence and citing to Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, & Rahul Chatterjee, *Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse*, 32 USENIX Security Symposium 69, 74-77 (Aug. 2023), https://www.usenix.org/system/files/usenixsecurity23-stephenson-vectors.pdf); CMU CR et al IoT Comment; EPIC, Success of FCC's IoT Cyber Trust Mark Depends Upon Meaningful Standards, Transparency, and Accountability (June 6, 2024), https://epic.org/success-of-fccs-iot-cyber-trust-mark-depends-upon-meaningful-standards-transparency-and-accountability/; EPIC IoT FNPRM Reply Comment.

[23] *See, e.g.*, Stephenson et al., *supra* note 22; CETA, The Technology Abuse Clinic Toolkit Ch 9: Helping with Tech Abuse, https://www.techabuseclinics.org/ch-9-helping-with-tech-abuse; Safe Connections FNPRM, *supra* note 6 at ¶¶ 6, 9, 13 (describing risks of abuse specific to connected cars); EPIC IoT FNPRM Reply Comment at 6 (citing to findings of FCC and of Congress as they relate to the Safe Connections Act).

[24] 47 U.S.C. § 154(n).

[25] Encouragingly, the Bureau has already taken action in this direction. *See, e.g.*, 2024 AT&T Vendor Breach Settlement. *See also* FCC Settles Data Breach Notification Case with Liberty Latin America (Rel. June 13, 2024), https://www.fcc.gov/document/fcc-settles-data-breach-notification-case-liberty-latin-america [hereinafter "Liberty Settlement"] (referring to *In re* Liberty Latin America Limited, et al., Order, File No.: EB-TCD-23-00035125).

[26] *See, e.g.*, 2023 Data Breach Reporting Order at ¶ 3 (noting telecommunications companies may be "particularly vulnerable" to breaches of personal information); 2024 AT&T Vendor Breach Settlement; Brian Krebs, *Hackers Claim They Breached T-Mobile More Than 100 Times in 2022*, Krebs on Security (Feb. 28, 2023), https://krebsonsecurity.com/2023/02/hackers-claim-they-breached-t-mobile-more-than-100-times-in-2022/; *Verizon Customer Data for Sale on Dark Web, New Data Breach Suspected*, https://thecyberexpress.com/verizon-customer-data-for-sale-on-dark-web/amp/ (Feb. 16, 2023); Lily Hay Newman, *T-Mobile's $150 Million Security Plan Isn't Cutting It*, Wired (Jan. 20, 2023), https://www.wired.com/story/tmobile-data-breach-again/; Brian Krebs, *It Might Be Our Data, But It's Not Our Breach*, KrebsOnSecurity (Aug. 11, 2022), https://krebsonsecurity.com/2022/08/it-might-be-our-data-but-its-not-our-breach/; Sergiu Gatlan,

Verizon notifies prepaid customers their accounts were breached, Bleeping Computer (Oct. 18, 2022), https://www.bleepingcomputer.com/news/security/verizon-notifies-prepaid-customers-their-accounts-were-breached/.

[27] *See, e.g.*, Br. of Amicus Curiae Electronic Privacy Information Center, Privacy Rights Clearinghouse, and Public Knowledge in support of the Federal Communications Commission and United States of America, *Ohio Telecom Association, et al. v. Fed. Commc'ns Comm'n and United States of America*, No. 24-3133 (6th Cir. Aug. 6, 2024), *available at* https://epic.org/documents/ohio-telecom-association-et-al-v-fcc-and-usa-data-breach-reporting-reqts/; Reply Comments of EPIC, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, *in re* Data Breach Reporting Requirements, WC Dkt. No. 22-21 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814.

[28] *See, e.g.*, all three enforcement orders cited, *supra* note 2; Liberty Settlement Consent Decree at 4 ¶ 8 (noting 201(b) extends to carriers' data security practices where carrier's vendor was breached); Cox Order (also citing to cable privacy authorities); *AT&T To Pay $25M To Settle Investigation Into Three Data Breaches*, DA 15-399, Order at ¶ 3, Consent Decree at ¶ 5 (Rel. Apr. 8, 2015), https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches; *in re TerraCom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175 at ¶¶ 2, 11, 12, 31-44 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1_Rcd.pdf [hereinafter "TerraCom NAL"]. Additionally, on multiple occasions Commissioner Starks has emphasized privacy and data security in the context of the Commission's 201(b) authority. *See, e.g.*, In re *Protecting Against Natl. Sec. Threats to the Commun. Supply Chain Through Fcc Programs*, 35 F.C.C. Rcd. 7821 (F.C.C. 2020) ("untrustworthy equipment that threatens our data privacy and network security cannot be managed or tolerated in any form"). *See also, In re Protecting Against Natl. Sec. Threats to the Commun. Supply Chain Through Fcc Programs Huawei Designation Zte Designation*, 34 F.C.C. Rcd. 11423 (F.C.C. 2019) ("…I have said many times that the untrustworthy equipment from these companies could readily serve as a 'front door' for Chinese intelligence gathering, at the expense of our privacy and national security."). There are numerous other examples of the Commission invoking 201(b) as a privacy authority. *See also* FCC Enforcement Advisory No. 2023-03, DA 23-1148, Telecommunications Carriers Must Protect Consumers' Privacy and Sensitive Data by Taking Reasonable Steps to Prevent SIM Fraud Schemes, at 2 n 7 (Rel. Dec. 11, 2023) (noting that allowing fraudulent SIM swaps can violate 201(b)); FCC Launches First-Ever Enforcement Partnerships with State Attorneys General (Rel. Dec. 6, 2023), https://www.fcc.gov/document/fcc-launches-first-ever-enforcement-partnerships-state-attorneys-general (announcing MOUs regarding enforcement of privacy, data protection, and cybersecurity issues under Sections 201 and 222); 2024 Title II Order at ¶¶ 68, 324, 359 n 1452 (citing to 201(b) as a privacy authority).

[29] Respondent Br. of FCC and USA, *Ohio Telecom Association, et al. v. Fed. Commc'ns Comm'n and United States of America, et al* No. 24-3133 at 16-17, 21-33 (6th Cir. July 29, 2024).

[30] *See, e.g., in re Q Link Wireless LLC and Hello Mobile Telecom LLC*, Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-22-00034450 (Rel. Jul. 28, 2023), https://www.fcc.gov/document/fcc-proposes-20m-fine-apparently-failing-protect-consumer-data; *in re Cellco Partnership d/b/a Verizon Wireless*, Order, File No.: EB-TCD-14-00017601 (Rel. Mar. 7,

2016), https://www.fcc.gov/document/fcc-settles-verizon-supercookie-probe; *in re Verizon, Compliance with the Commission's Rules and Regulations Governing Customer Proprietary Network Information*, Adopting Order, File No.: EB-TCD-13-00007027 (Rel. Sept. 3, 2014), https://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation.

[31] *Gonzales v. Oregon*, 546 U.S. 243, 259 (2006) (citing to *Natl. Cable & Telecomm. Ass'n v. Brand X Internet Services*, 545 U.S. 967, 980 (2005)).

[32] FCC-FTC Consumer Protection Memorandum of Understanding (Nov. 16, 2015), https://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf.

[33] In its 2014 NAL against TerraCom and YourTel, the Commission stated: "carriers are now on notice that in the future we fully intend to assess forfeitures for [Section 201(b) data security and consumer notification] violations." TerraCom NAL, *supra* note 28 at ¶ 53. The Commission also noted that "proprietary information", of which CPNI is a subset, encompasses "all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or reasons of personal privacy." *Id.* at ¶¶ 14-15.

[34] This explicitly includes information beyond CPNI. *See, e.g.*, 2024 T-Mobile Settlement, *supra* note 2, at ¶¶ 1-3 (noting failure to meet duty to protect the confidentiality of customer proprietary information (PI) in violation of Sections 201(b) and 222); 2024 TracFone Settlement, *supra* note 2, at ¶¶ 1, 4, 6 (same); 2024 AT&T Vendor Breach Settlement, *supra* note 2, at ¶¶ 1, 3 (same); *see also* TerraCom NAL, *supra* note 28, at ¶ 12 (companies collected consumers' PI through their websites and failed to employ reasonable practices to safeguard this information); *id.* at ¶ 28 (finding a plain and practical reading of 222(a) requires the Commission to interpret Section 222(a) to protect an applicant's proprietary information); *in re* Quadrant Holdings LLC, Q Link Wireless LLC, and Hello Mobile LLC, File No.: EB-TCD-21-00032935 at ¶ 10 n 25 (F.C.C. Aug. 5, 2022) ("[t]he scope of "proprietary information" covered by section 222 extends beyond CPNI data to include private or sensitive data that a customer would normally wish to protect"); *in Re* China Unicom (Americas) Operations Ltd., FCC 22-9 at ¶¶ 83-85 (F.C.C. Feb. 2, 2022) ("The Commission expressed concern…that CUA's service offerings provide CUA with access to both customer PII and CPNI…") (internal citations omitted); *In re* P. Networks Corp. and Comnet (Usa) LLC, 37 F.C.C. Rcd. 6368 (F.C.C. 2021) (similar language as China Unicom order).

[35] *See, e.g.*, Comments of EPIC, et al., Federal Trade Commission, *in re Rule on Impersonation of Government and Business (SNPRM)*, FTC-2023-0030-0074 at 4-9 (Apr. 2024), https://epic.org/documents/epic-and-partner-organizations-comments-on-ftc-rule-on-impersonation-of-government-businesses-and-individuals-snprm/.

[36] *See, e.g.*, 2024 AT&T Vendor Breach Settlement, *supra* note 2, at ¶ 3. The Commission similarly notes this in each of its long-awaited orders related to location data. *See, e.g.*, *In re* AT&T Inc., Forfeiture Order, File No.: EB-TCD-18-00027704 at ¶ 7 (Rel. Apr. 29, 2024), https://www.fcc.gov/document/fcc-fines-largest-wireless-carriers-sharing-location-data; *see also* i*n re* Sprint Corporation, Forfeiture Order, File No.: EB-TCD-18-00027700 at ¶ 7 (Rel. Apr. 29, 2024); i*n re* T-Mobile USA, Inc., Forfeiture Order, File No.: EB-TCD-18-00027702 at ¶ 7 (Rel. Apr. 29,

2024); i*n re* Verizon Communications, Forfeiture Order, File No.: EB-TCD-18-00027698 at ¶ 7 (Rel. Apr. 29, 2024).

[37] *See, e.g.*, *In re AT&T Services Inc. and AT&T Corp. v. 123.Net, Inc. d/b/a Local Exchange Carriers of Michigan and/or Prime Circuits*, Memorandum Opinion and Order, EB-19-MD-007 at ¶ 3 (June 24, 2020), https://www.fcc.gov/ecfs/document/0624022185625/1 (discussing previous Commission orders holding that a carrier's statutory duties are non-delegable, including when performed by independent contractors); *see also in re* 911 Governance and Accountability, Improving 911 Reliability, Policy Statement and Notice of Proposed Rulemaking, PS Dkt. Nos. 14-193, 13-75 at ¶¶ 17-18 (Nov. 21, 2014), https://www.fcc.gov/ecfs/document/60000984124/6 (contracting out certain aspects of service provider's functions does not absolve individual entities of their respective 911 obligations).

[38] *See, e.g.*, *Champion v. Credit Pros Intl. Corp.*, No. CV2110814JXNJBC, 2022 WL 3152657 at *3-4 (D.N.J. Aug. 5, 2022); *Spurlark v. Dimension Serv. Corp.*, No. 2:21-CV-3803, 2022 WL 2528098 at *5 (S.D. Ohio July 7, 2022); *Alvord v. Quick Fi Capital Inc.*, No. 2:19-CV-000459-DB, 2019 WL 5788572 at *3 (D. Utah Nov. 6, 2019).

[39] *See in re* Protecting Consumers from SIM Swap and Port-Out Fraud, Report and Order and Further Notice of Proposed Rulemaking, WC Dkt. No. 21-341 at ¶ 25 n. 93 (Rel. Nov. 16, 2023), https://docs.fcc.gov/public/attachments/FCC-23-95A1.pdf (noting that the obligations of CMRS providers, treated as common carriers, apply to agents or other persons acting for or employed by the CMRS provider acting within the scope of their employment).

[40] *See in re* Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform Modernization, Affordable Connectivity Program, Report and Order, WC Dkt. Nos. 22-238, 11-42, 21-450 at ¶ 43 (Rel. Nov. 16, 2023), https://docs.fcc.gov/public/attachments/FCC-23-96A1.pdf [hereinafter "Safe Connections Order"] (covered providers liable for "failures by their vendors, agents, and contractors to adopt sufficient confidentiality and secure disposal measures").

[41] *See in re* Rural Call Completion, Second Report and Order and Third Further Notice of Proposed Rulemaking, WC Dkt. No. 13-39 at ¶ 24 (Rel. Apr. 17, 2018), https://docs.fcc.gov/public/attachments/FCC-18-45A1.pdf (in the context of rural call completion, carrier liable for underlying provider's violations of Section 201 where underlying provider is agent or acting for or employed by carrier); Letter to Hon. Vicky Hartzler from FCC Chair Wheeler at digital page 5 of 25 (Dec. 11, 2013), https://www.fcc.gov/ecfs/document/6017582922/5 (carriers liable for Lifeline fraud committed by agents, contractors, or representatives).

[42] *See* Comments of Public Knowledge and Consumer Reports, *in re* Improving Competitive Broadband Access to Multiple Tenant Environments, GN Dkt. No. 17-142 at 18 (Oct. 20, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/102048893676.

[43] *See, e.g.*, *In re* Location-Based Routing for Wireless 911 Calls, Report and Order, PS Dkt. No. 18-64 (Rel. Jan. 26, 2024), https://docs.fcc.gov/public/attachments/FCC-24-4A1.pdf; *In re* Facilitating Implementation of Next Generation 911 Services (NG911), Location-Based Routing for Wireless 911 Calls, Report and Order, PS Dkt. Nos. 21-479, 18-64 (Rel. July 19, 2024), https://docs.fcc.gov/public/attachments/FCC-24-78A1.pdf.

[44] *See, e.g.*, Reply Comments of Electronic Privacy Information Center, *In re* Implementation of the National Suicide Hotline Act of 2018, WC Dkt. No. 18-336 at 13 (July 29, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10729418918342 [hereinafter "EPIC 988 Reply Comments"] ("As the Commission's implementation of the Safe Connections Act prohibited calls made by survivors of intimate partner violence to be used to inform marketing programs, so too should the Commission's implementation of the National Suicide Hotline Act of 2018 prohibit calls made to 988 from being used for any purposes other than connecting the call to the appropriate local crisis hotline.") (internal citations omitted); Fact Sheet, Implementation of the National Suicide Hotline Act of 2018, Third Report and Order and Third Further Notice of Proposed Rulemaking, WC Dkt. No. 18-336 at ¶ 70 (Rel. Sept. 26, 2024), https://docs.fcc.gov/public/attachments/DOC-405823A1.pdf (noting that "protecting the privacy and security of callers is imperative…wireless providers must aggregate location data generated from cell-based technology to a sufficiently granular level to maintain caller privacy").

[45] *See, e.g.*, Safe Connections Order, *supra* note 40; Reply Comment of EPIC, Clinic to End Tech Abuse (CETA), National Network to End Domestic Violence, and Public Knowledge, *in re* Supporting Survivors of Domestic and Sexual Violence, WC Dkt. No. 22-238 at 5-8 (June 24, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1062570060032; CMU CR et al IoT Comment, *supra* note 6 at 4-5; EPIC IoT FNPRM Reply Comment, *supra* note 7, at 6.

[46] *See, e.g.*, *In re* AT&T Inc., File No.: EB-TCD-18-00027704, Statement of Comm'r Geoffrey Starks at 42 (Feb. 28, 2020), *available at* https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf ("But that is no excuse for failing to conduct a comprehensive investigation—including issuing subpoenas to Securus—of the events in question here. That information would have enriched our investigation and could have been provided to other agencies for investigation and enforcement.").

[47] *Id.* at 41 ("despite the extraordinary length of our investigation, we let this problem fester for too long… Even with the reduced redactions, Americans who read these Notices and the news coverage of them today will not have all the facts to which they are entitled. So while I am glad that we are ordering the parties to explain why we should not deny their requests completely, I worry that the carriers will have succeeded in hiding key facts until the spotlight has moved on. The FCC must do better.").

[48] *See, e.g.*, Forum on Geolocation for 988 (May 24, 2022), https://www.fcc.gov/news-events/events/2022/05/forum-geolocation-988; FCC Announces Tribal Consultation on Proposed Missing and Endangered Persons Emergency Alert System Code (Apr. 30, 2024), https://www.fcc.gov/sites/default/files/onap_eblast_tribal_consultation_MEP-Code_2024.pdf.

[49] EPIC 988 Reply Comments, *supra* note 44, at 19-20 ("However, it would be a particularly cruel distortion of that authority for the Commission to use it to dispatch unwanted assistance to someone who may actually be significantly worse off as a result of the dispatched 'help.' ")