Before the

Federal Communications Commission

In the Matter of:

Supporting Survivors of Domestic and Sexual Violence
89 Fed. Reg. 30,303, WC Docket No. 22-238

Further Notice of Proposed Rulemaking

Comment of

Electronic Privacy Information Center (EPIC), and

Public Knowledge

May 23, 2024

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Harold Feld
Senior Vice President
Public Knowledge
1818 N Street, NW, Suite 410
Washington, DC 2003

Summary

Electronic Privacy Information Center (EPIC) and Public Knowledge file these comments to support the Commission's efforts to better protect survivors of domestic violence by reducing the opportunities available to abusers to control, surveil, or revictimize survivors by misusing America's communications systems. We re-iterate and expand upon the core principles that should guide the Commission throughout this proceeding (Section II), and which have been supported by numerous other civil society organizations as noted in our contemporaneous, shorter coalition comment filing.

EPIC and Public Knowledge urge the Commission to avoid creating loopholes (Section III) that can result in dangerous gaps that expose survivors to continued risk and chill their participation in programs due to their uncertainty about being protected; the Commission should also strive to answer a few clarifying questions about implementation of its proposals.

In terms of Commission actions (Section IV), we urge the Commission to define terms like "victim services provider" in a manner that aligns with the five core principles, to require privacy and cybersecurity controls that are tailored to the unique risks and needs faced by survivors, and to demand transparency from its private sector partners.

Although the Commission has authority under the Safe Connections Act (SCA) (Section V), we argue the Commission also has multiple adequate authorities beyond the SCA (Section VI) to implement its proposals (and any similar proposals) to prevent misuses of the American communications system in ways that result in increased risks to the personal safety of survivors.

Table of Contents

I. Introduction

The **Electronic Privacy Information Center (EPIC)**[1] and **Public Knowledge**[2] submit these comments to the Federal Communications Commission (FCC or Commission) regarding supporting survivors of domestic and sexual violence (hereinafter domestic violence) through its continued implementation of the Safe Connections Act (hereinafter SCA or the Act), per the Further Notice of Proposed Rulemaking (FNPRM) published in the Federal Register on April 23, 2024.[3]

We were encouraged to see Chairwoman Rosenworcel[4] and the Commission[5] act so rapidly in response to reading news articles about the threats connected car services can pose to survivors.

In these comments, we urge the Commission to:

- Adhere to five core principles, also supported by a coalition of advocates as evidenced in our contemporaneous coalition filing;
- Address implementation issues, including offering clarifications and avoiding the creation of loopholes;
- Take action to protect survivors by defining terms in ways that align with the five core principles, by requiring privacy and cybersecurity controls that meet the unique risks and needs of survivors, and by demanding transparency from providers; and
- Articulate the full breadth of its authority to implement these and similar proposals under the Safe Connections Act and the Commission's many other relevant authorities.

II. The Commission should continue to advance five core principles to promote survivor safety.

As we noted in our initial NPRM comments, the Commission should uphold the principles of: maximizing survivor self-determination and agency, minimizing burdens to

[1] EPIC is a public interest research center in Washington, DC seeking to protect privacy, freedom of expression, and democratic values in the information age.

[2] Public Knowledge is a nonprofit advocacy group that promotes freedom of expression, an open internet, and access to affordable communications tools and creative works.

[3] *In Re: Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238, Further Notice of Proposed Rulemaking, FCC 24-38, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence [hereinafter "FNPRM"].

[4] *See* Press Release, *Chairwoman on Safe Connected Cars for Domestic Violence Survivors* (Jan. 11, 2024), https://www.fcc.gov/document/chairwoman-safe-connected-cars-domestic-violence-survivors.

[5] *See* Further Notice of Proposed Rulemaking, *In Re: Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238 (Rel. Apr. 8, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1040883948778.

survivors to maximize program utilization, and prioritizing data minimization and data security.[6] As we discuss in our coalition letter filed contemporaneously with this comment in response to this FNPRM, in the context of connected car systems, two additional principles also apply: proactively preventing misuse and putting access burdens on providers and manufacturers, not on survivors.[7] These points are consistent with the Commission's R&O in this docket[8] and with our comments to the FCC regarding concerns for survivors in the context of the Commission's U.S. Cyber Trust Mark IoT cybersecurity labels.[9]

a. Connected car systems should support survivor self-determination and agency.

Survivors are best positioned to know their own immediate needs and safety risks. As Commissioner Starks has observed: "One refrain from those meetings was consistent—empowering survivors to reach out when and how they see fit is a key part to supporting them as they look for a fresh start."[10] Deleting or obscuring data, including effectuating a line separation request, could increase the risk of imminent physical violence to the survivor. While secure communications are an essential step to achieving independence from an abuser, it must be up to the survivor when and how to take advantage of the options available to protect them. However, some design changes are likely to be universally valuable to survivors, see section e, *infra*.

The Commission's Report and Order has advanced the principle of survivor self-determination and agency through its prioritization of survivor flexibility,[11] including by allowing survivors to provide a recent address rather than a current address.[12] Prioritization of survivor access/program utilization also reflects this principle see section b, *infra*.

In response to the Commission's question about how its proposals may best serve survivors experiencing compounded vulnerabilities (including individuals who identify with

---

[6] *See* Comments of Electronic Privacy Information Center (EPIC) et al., WC Docket Nos. 22-238, 11-42, 21-450 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/104131354805768 [hereinafter "EPIC NNEDV et al. NPRM Comments"].

[7] *See* Coalition Comments of Electronic Privacy Information Center (EPIC) et al., WC Docket No. 22-238 (May 23, 2024), link not yet available. These points are also consistent with our comments to the Commission regarding concerns for survivors of intimidate partner violence (IPV) in the Commission's IoT cybersecurity labels. *See* Reply Comments of EPIC, Clinic to End Tech Abuse, Madison Tech Clinic, Public Knowledge, and Ranking Digital Rights, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 23-26 (Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111054758013 [hereinafter "EPIC et al. IoT Reply Comments"].

[8] Report and Order, *In Re: Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform Modernization, Affordability Connectivity Program*, WC Docket Nos. 22-238, 11-42, 21-450 (Rel. Nov. 16, 2023), https://docs.fcc.gov/public/attachments/FCC-23-96A1.pdf [hereinafter "R&O"].

[9] *See* EPIC et al. IoT Reply Comments at Section III(B)(III)(b)(3).

[10] Statement of Comm'r Geoffrey Starks, *In Re:* Lifeline and Link Up Reform and Modernization, WC Docket No. 11-42; *Affordable Connectivity Program*, WC Docket No. 21-450; *Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238, Notice of Inquiry (July 14, 2022), https://docs.fcc.gov/public/attachments/FCC-22-56A3.pdf.

[11] *See, e.g.*, R&O at ¶ 64.

[12] *See, e.g.*, R&O at ¶ 169.

historically marginalized demographics),[13] we reiterate that a flexible approach to how a survivor can benefit from these protections will advance this goal better than a prescriptive approach.[14] There is not a singular way to safely escape from an abusive relationship, and the Commission should not intentionally or unintentionally create one, especially not in ways that will have inequitable impacts.

b. The Commission should prioritize program utilization and accessibility over hypothetical fraud concerns.

We encourage the Commission to make its protections as accessible as possible to survivors, although we recognize that fraud and abuse concerns with line separation in the context of a vehicle may be different from these concerns with line separation in the context of a phone plan. In the case of a phone plan, commenters' concerns seemed largely focused on non-survivors falsely claiming to be survivors in order to enjoy temporarily discounted phone service. In the case of a vehicle, fraud and abuse concerns could impact access to valuable property with further implications for safety (e.g., an abuser could leverage the very measures designed to protect survivors to instead deprive a survivor of vehicle features, or a thief could use the line separation process to delay recovery of a stolen vehicle). We offer our recommendations and rationale further below, but in short: survivor safety should be paramount, and the Commission should not disregard these fraud concerns, but we urge the Commission to prioritize supporting survivors, even at the risk of complicating paths to relief for others.[15]

The Commission has some leeway in making its programs offered under the Safe Connections Act more accessible to survivors. As we have articulated in this docket already,[16] and as the National Academies recently reported,[17] there are several reasons why a survivor may

---

[13] *See, e.g.*, FNPRM at ¶ 25, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-43.

[14] For example, allowing for self-certification rather than requiring a third party such as law enforcement or a service provider to "vouch" for the survivor. *See, e.g.*, EPIC NNEDV et al. NPRM Comments at 8–9 ("Self-certification is preferable to third-party certification, which imposes barriers for survivors. Many survivors never actually seek services. This includes but is not limited to LGBTQ+, indigenous, immigrant, Asian-American, Jewish, and male survivors, as well as survivors experiencing financial insecurity. Survivors in rural areas may need to traverse three times the distance to reach the nearest supportive services program. Requiring third-party certification would predictably result in inequitable access to the Commission's programs.") (internal citations omitted).

[15] The Commission has had to balance equities similarly in its 2007 CPNI order in response to pretexting attacks used to obtain subscriber information for nefarious purposes. *See in re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network information and Other Customer Information, IP-Enabled Services*, 22 F.C.C.R. 6927 (2007) [hereinafter "Pretexting Order"].

[16] *See, e.g.*, EPIC NNEDV et al. NPRM Comments at 2-3; *In re: Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program*, Comments of EPIC et al. on Notice of Inquiry, WC Docket Nos. 22-238, 11-42, 21-450 at 2–5 (Aug. 18, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/1081899226693.

[17] *See, e.g.*, National Academies of Science, Engineering, and Medicine, *Essential health care services addressing intimate partner violence*, National Academies Press at 45, 48, 53-55 (2024), https://nap.nationalacademies.org/read/27425/chapter/4#45.

be reluctant to engage law enforcement, the courts, or even clinicians. The Commission should not foist this requirement upon survivors—except to the extent they serve as necessary safeguards for the personal safety of a survivor. Requiring a court order means engaging a court; requiring a police report means engaging law enforcement. As we argue in Section III, *infra*, the Commission can take advantage of the opportunity to clarify undefined terms to hew more closely to the principle of prioritizing program utilization and accessibility. The record supports the principle of survivor autonomy and prioritization of program utilization,[18] and there are numerous examples in the R&O in which the Commission has already advanced this principle.[19]

c. Connected car systems should implement data minimization and data security by default.

The Commission should ensure that a survivor can feel confident that they are in control of who is able to access their data, both presently and in the future. A survivor should not be concerned about a future data breach exposing historical data about them, and data minimization is key to providing this assurance. Data minimization safeguards should include periodic deletion of data and an easy process for a driver to manually prevent their data from being collected or shared or to manually delete their data after the fact. Where a car collects data under different user accounts, data should not be accessible across accounts (i.e., User B should not be able to access User A's data).

In a recent Kaspersky survey, 87% of participants indicated that automakers should be required to delete a user's data upon request.[20] 71% of respondents indicated they would consider buying an older car or one with less technology to protect their privacy and security, yet "both of these options are likely to get less realistic as time goes on and connected cars make up a growing share of the available inventory."[21]

The Commission should be wary of industry attestations of the effectiveness of self-regulation. The industry's published privacy principles that the Federal Trade Commission ("FTC") once called an "important step"[22] seem to be at odds with the realities uncovered in

---

[18] *See, e.g.*, Reply Comments of EPIC et al., *In re:* Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program, WC Docket Nos. 22-238, 11-42, 21-450 at 1–3 (May 21, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10512158610690 [hereinafter "EPIC et al. Reply Comments"].

[19] *See, e.g.*, R&O at ¶ 26; id. at ¶ 164 (allowing self-certification of financial hardship); *id.* at ¶ 34 (prohibiting from assessing veracity of survivor status, reasonable reliance on documentation provided); *id.* at ¶ 45 (maximizing simplicity); *id.* at ¶ 53 (utilization); *id.* at ¶ 62 (easily navigable).

[20] Kaspersky, *Is my car spying on me?*, at 2 (Jan. 2024), https://media.kasperskydaily.com/wp-content/uploads/sites/85/2024/01/10103616/13195_Driver_Survey_Report_WEB-2.pdf.

[21] *Id.* at 3.

[22] Staff Perspective, *Connected Cars Workshop*, Fed. Trade Comm'n 3 (Jan. 2018), https://www.ftc.gov/system/files/documents/reports/connected-cars-workshop-federal-trade-commission-staff-perspective/staff_perspective_connected_cars_0.pdf (referring to Alliance for Automative Innovation, Inc., Consumer Privacy Protection Principles (est. Nov. 12, 2024, rev. May 2018, Mar. 2022), https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf).

Mozilla's recent reporting[23] and in recent vulnerability disclosures.[24] The auto industry has suffered multiple breaches recently.[25] Even the industry letters submitted to the Commission in response to Chairwoman Rosenworcel's inquiries must be carefully parsed,[26] and may still prove to contain outright misrepresentations.[27]

Furthermore, even if industry privacy policies were generally effective, they would not address the specific problems facing abuse survivors. As with family plan phone contracts, the threat is not always an outsider accessing information but frequently involves a party to the ownership or lease of the car. Adequately addressing this threat requires the Commission to create rules that override standard industry practices and standard contractual arrangements where an abuser is a party to the contract—or even the primary owner on the title or lease. Only the force of law—through the Commission's regulations—can both compel automobile manufacturers to protect the location and personal information of domestic abuse survivors and immunize the manufacturers from any subsequent legal action by the abuser.

As we discuss in Section VI, *infra*, the Commission has the authority to ensure the safe, secure functioning of our nation's communications infrastructure, including the privacy of the

---

[23] *See* Jen Caltrider, Misha Rykov, and Zoe MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, *Privacy Not Included (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[24] *See, e.g.*, Jonathan M. Gitlin, *Hackers discover that vulnerabilities are rife in the auto industry*, ArsTechnica (Jan. 11, 2023), https://arstechnica.com/cars/2023/01/hackers-discover-that-vulnerabilities-are-rife-in-the-auto-industry/ ("Armed with nothing more than a vehicle identification number, the hackers were able to access the remote services"; "…vehicles were similarly exploitable, albeit with an owner's email address instead of a VIN").

[25] *See, e.g.*, Zach Whittaker, *Toyota confirms another years-long data leak, this time exposing at least 260,000 car owners*, TechCrunch (May 13, 2023), https://techcrunch.com/2023/05/31/toyota-customer-data-leak-years/; Avast Security News Team, *Hacker breaches GPS service of 27,000 cars*, Avast Blog (Apr. 27, 2019), https://blog.avast.com/hacker-breaches-gps-service-of-27000-cars; Lee Mathews, *Data From 540,000 GPS Vehicle Trackers Leaked Online*, Forbes (Sept. 22, 2017), https://www.forbes.com/sites/leemathews/2017/09/22/data-from-540000-vehicle-tracking-devices-leaked-online/?sh=720e3544274b.

[26] *See, e.g.*, Letter, Hyundai Motor America, WC Dkt. No. 22-238 at 2 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10227310026275 ("HMA does not operate as an MVNO. Wireless data services are provided by HAEA as described above.").

[27] *See, e.g.*, Letter, American Honda Motor Co., WC Dkt. No. 22-238 at 5 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/102271630118952 ("In 2023, Honda did not receive direct monetary compensation in exchange for vehicle data disclosed without consumer consent to third parties who are not its service providers"); "Honda," *Privacy Not Included (review date Aug. 15, 2023), https://foundation.mozilla.org/en/privacynotincluded/honda/ ("We disclose Covered Information to third parties who provide goods or services that may benefit vehicle owners, including insurance companies, Honda/Acura dealerships, and consumer goods or services companies, such as satellite radio providers and connected vehicle data services and analytics platforms. These companies may use Covered Information for their everyday business purposes, *including marketing*, customer service, fulfillment and related purposes. *These disclosures may qualify as a sale under certain state privacy laws*.") (emphasis added).

data collected as part of those communications.[28] Additionally, the Commission's cybersecurity equities are not limited to concerns of national security but also include personal safety. The Commission should continue[29] to work with the FTC, which is also looking into these troubling industry practices, including the role of data brokers.[30]

Notice and choice models of consent are not effective as a general matter,[31] but specifically in the context of survivor privacy, consent can be coerced during installation or initial setup.[32] As a result, checks for consent should be periodic and randomized. If the frequency with which a renewed request for consent appears is predictable, abusers may anticipate this routine and ensure the survivor never gets an opportunity to disable or even be

[28] *See, e.g.*, "Protecting Your Personal Data", Fed. Commc'ns Comm'n, https://www.fcc.gov/protecting-your-personal-data; "Privacy/Data Security/Cybersecurity: Customer Proprietary Network Information", Fed. Commc'ns Comm'n, https://www.fcc.gov/enforcement/areas/privacy; "Privacy and Data Protection Task Force," Fed. Commc'ns Comm'n, https://www.fcc.gov/privacy-and-data-protection-task-force ("The FCC has an important role to play ensuring the privacy of consumer communications").

[29] *See, e.g.*, Comments of EPIC, Public Knowledge, Consumer Federation of America, and Demand Progress Education Fund, *In re: Safeguarding and Securing the Open Internet*, WC Dkt No. 23-320 at 6, 10-12 (Dec. 14, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1215730424019 [hereinafter "EPIC et al. Open Internet Comments"].

[30] *See, e.g.*, *Cars & Consumer Data: On Unlawful Collection & Use*, Technology Blog (May 14, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use; Press Release, *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data* (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data ("company sold precise location data that could be used to track people's visits to sensitive locations such as medical and reproductive health clinics, places of religious worship and domestic abuse shelters"). We further note that information from data brokers can be leveraged by abusers to stalk, harass, or otherwise surveil, control, or otherwise attempt to revictimize survivors, as the FCC is well aware. *See, e.g.*, Joseph Cox, *Stalkers and Debt Collectors Impersonate Cops to Trick Big Telecom Into Giving Them Cell Phone Location Data*, Motherboard (Mar. 6, 2019), https://www.vice.com/en/article/panvkz/stalkers-debt-collectors-bounty-hunters-impersonate-cops-phone-location-data; *see also* Cyber Policy and Gender Violence Initiative, *Privacy Issues From Data Brokers*, Duke Sanford School of Social Policy, https://sites.sanford.duke.edu/genderviolencepolicy/privacy-issues-for-gender-violence-survivors/.

[31] *See, e.g.*, Remarks of Samuel Levine, *Toward a Safer, Freer, and Fairer Digital Economy*, Fourth Annual Reidenberg Lecture Fordham Law School (Apr. 17, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/20240417-Reidenberg-Lecture-final-for-publication-Remarks-Sam-Levine.pdf.

[32] *See, e.g.*, "Stalkerware: Phone Surveillance & Safety for Survivors," National Network to End Domestic Violence Safety Net Project, https://www.techsafety.org/spyware-and-stalkerware-phone-surveillance ("Almost all phone stalkerware requires physical access to the device to install. Once installed, it runs in stealth mode without any notification or identifying activity and is difficult to detect or remove.").

made aware of the surveillance.[33] (This also relates to sections d and e, *infra.*) In their response letters, car companies rely heavily upon consent.[34]

The Commission's Report and Order has already advanced the principle of data minimization and data security through its treatment of confidentiality and disposal requirements.[35]

Companies are clearly capable of thinking through and implementing privacy-friendly designs.[36] This kind of product design thinking should be employed in the context of survivor safety as well, as we discuss further immediately below.

d. Connected car systems should proactively prevent misuse.

The Commission asks "what steps connected car service providers can proactively take to protect survivors from being stalked, harassed, intimidated, or otherwise revictimized through the misuse of connected car service."[37] Proactively preventing misuse, such as through process or product design choices, can protect survivors universally, including those who do not engage in supportive services (either by choice or out of necessity).[38]

These changes might include delayed notification, as the Commission has already proposed.[39] Persistent visual notification that location information is being stored or shared is also likely to be a universally helpful design feature.[40] The ability for someone in the vehicle to override any remote control or tracking also seems universally beneficial to survivors.[41] Design

---

[33] *See, e.g.*, EPIC et al. Reply Comments at 7.

[34] *See, e.g.*, Letter, Tesla, WC Dkt. No. 22-238 at 4 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10227291877863; Letter, Stellantis North America, WC Dkt. No. 22-238 at 1 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10227024186428; Letter, Nissan North America, Inc., WC Dkt. No. 22-238 at 2 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1022716263709.

[35] *See, e.g.*, R&O ¶¶ 41–44.

[36] *See, e.g.*, Letter, Tesla, at 1 (discussing differential privacy).

[37] FNPRM at ¶ 2, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-20.

[38] For example, due to inability to access quality resources. *See* National Academies, *supra* note 17, at 47, https://nap.nationalacademies.org/read/27425/chapter/4#47.

[39] *See* FNPRM at ¶ 23, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-41.

[40] *See, e.g.*, Letter, Tesla, *supra* note 34, at 2 (describing arrow icon persistently displayed when vehicle's live location is requested by an app).

[41] *See, e.g.*, EPIC et al. IoT Reply Comments at 24; Letter, Ford Motor Company, WC Dkt. No. 22-238 at 2 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1022768491579; Letter, General Motors Company, WC Dkt. No. 22-238 at 2 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1022787068517; David Ruiz, *Why car location tracking needs an overhaul*, Malwarebytes Labs (May 13, 2024), https://www.malwarebytes.com/blog/privacy/2024/05/why-car-location-tracking-needs-an-overhaul ("According to Reuters, the roadside assistance service OnStar, which is owned by General Motors, allows any car driver—be they a vehicle's owner or not—to hide location data from other people who use the same vehicle.").

changes could also include features that some providers already purport to offer such as granular user controls.[42] Solutions being implemented in other sectors could also be relevant in the context of connected car services, for instance detecting potential surveillance equipment.[43] We note that one recent IoT device security standards specification requires that the device manufacturer document expected customers and use cases "including known potential misuses."[44]

Some industry education may be necessary here. For example, not only real-time location data poses a significant threat to survivors[45]—historical location data can also be dangerous in the hands of an abuser.

Special attention must be paid to purported consent where domestic violence is concerned. Abusers have been known to create a paper trail that suggests their intended victim willingly made decisions that are actually to the survivor's detriment.[46] As discussed in section c *supra*, in the context of data collection, consent must be collected periodically, and ideally on a randomized basis.

The Commission's Report and Order has already advanced this principle through its requirement to inform survivors in advance about the date upon which an abuser will be notified about the line separation request.[47]

e. The burden of accessing survivor services should be on manufacturers and providers, not on survivors.

Survivors are likely navigating imminent threats to their personal safety; are subjected to events, thoughts, or feelings that trigger trauma responses; and may be uprooting their lives in the interest of their continued safety and the continued safety of their children or other loved ones. In recognition of this challenging reality faced by survivors, the burden should be on providers as much as possible to make their features are easy to use or active by default, rather than putting the burden on survivors to be aware of—and to find the time, energy, and technological expertise to take advantage of—these programs or features. This final principle is

[42] *See, e.g.*, Letter, Ford Motor Company, at 2 (describing ability to turn off location data without having to also turn off vehicle health alerts).

[43] *See, e.g.*, Jennifer Pattison Tuchy, Apple finally adds iPhone alerts for third-party Bluetooth trackers, The Verge (May 13, 2024), https://www.theverge.com/2024/5/13/24155630/apple-google-airtag-bluetooth-tracker-alert-standard..

[44] Connectivity Standards Alliance, *IoT Device Security Specification Version 1.0* at 22, Standard 6.1.1 (Mar. 18, 2024), https://csa-iot.org/wp-content/uploads/2024/03/23-80986-013-PSWG-1.0-Specification-18-March-2024.pdf.

[45] *See, e.g.*, Letter, Toyota Motor North America Inc., WC Dkt. No. 22-238 at 3 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1022768491579.

[46] For example, coerced debt. *See, e.g.*, "Coerced Debt", National Consumer Law Center, https://www.nclc.org/topic/coerced-debt/.

[47] *See, e.g.*, R&O at ¶ 77.

closely related to the principles of prioritizing program utilization and proactively preventing misuse.

This kind of burden-shifting includes reducing the hoops that a survivor must jump through in order to benefit from supportive services (e.g., not requiring extensive documentation) and eliminating any strings attached to those services that may chill survivor utilization (e.g., ensuring there are no additional charges, that signing up for a support program will not result in unwanted marketing communications, etc.). This also includes raising awareness of the programs and features that can help protect a survivor, rather than leaving it to the survivor to read it in an instruction manual or by some other cumbersome method.

To the maximum extent possible, solutions should be available universally, to reduce the risk that a survivor believes that they are benefiting from a protection when in reality—due to some quirk of the underlying technology or corporate structure or other reason—the survivor is actually still exposed to risk. This is obviously dangerous in the immediate moment but in the long term could also result in reduced survivor utilization of beneficial programs or features due to uncertainty about whether they will actually protect the survivor. We discuss this further in Section V(b), *infra*.

The Commission's Report and Order has already advanced this principle by maximizing the ease with which survivors can obtain timely line separation,[48] ensuring the process for requesting line separation is easily navigable and in a language the survivor can understand,[49] and directing USAC to give survivors advanced notice that their temporary support is ending.[50]

The Commission should prioritize the safety and well-being of individuals who are subject to novel forms of monitoring and abuse because of connected car systems and enact policies that incentivize providers to prioritize the same.

III. The Commission should be mindful of implementation challenges and prevent exploitation of loopholes.

The Commission should be mindful to clarify both the intentions and the consequences of its proposals in developing the record in this proceeding; to adequately forecast implementation challenges; and to avoid unintentionally creating loopholes that leave survivors exposed to preventable risk. At a minimum, these should include being explicit about the consequences of line separation, directly addressing questions of ownership, ensuring providers fully understand and comply with their obligations to avoid creating uncertainty amongst survivors, identifying other relevant stakeholders in the connected car ecosystem, identifying other agencies the Commission may need to partner with to ensure compliance, and articulating what differences if any the Commission may have between its expectations for connected car service providers and other service providers. We do not mean to slow this proceeding: where the Commission can come to determinations, it should implement them in an order without delay. But where further

[48] *See, e.g.*, R&O at ¶ 45.

[49] *See, e.g.*, R&O at ¶¶ 62–63.

[50] *See, e.g.*, R&O at ¶ 177.

development of the record is necessary, the Commission should continue to issue successive further notices of proposed rulemaking.

One of the first things the Commission should seek to clarify in this proceeding is what exactly the consequences may be for line separation in the context of connected car services. Processes devised to protect survivors can be implemented instead by abusers to the detriment of survivors, and the Commission should anticipate this. For example, if no proof is required for line separation, and this can result in a survivor being unable to access the vehicle they rely upon or being unable to utilize essential functionality of that vehicle,[51] the Commission should re-evaluate its proposal.[52] However, if line separation merely results in the survivor being unable to access the data of the abuser, this seems significantly less problematic. Similarly, it is unclear at present whether line separation can only be effectuated where there are multiple vehicles, each with its own number, or whether multiple accounts associated with same vehicle could also be subject to separation. Also, is this regulation intended only to support survivors who have already achieved some measure of legal protection from their abusers and therefore prevent continued stalking and harassment post-separation? Or is it the Commission's intention to protect survivors who may still, for example, share a residence with their abuser and require these protections in order to safely engage supportive services in the first instance? We acknowledge that such boundaries are not always necessarily clear.

The Commission should not shy away from questions of ownership and property interests. While at its core this isn't a matter of property rights and ownership of the vehicle—this is a matter of individual safety and freedom from surveillance and control—the proceeding does touch upon property interests. A court order shouldn't be necessary where the survivor is seeking safety and freedom from surveillance and control but not a property interest in the vehicle.[53] However, where the survivor is seeking sole control of their vehicle, a court order or proof of ownership is likely necessary.

Survivors should not be left to guess whether the connected car they are using includes a provider who is not subject to the Commission's rules;[54] this is especially important in the context of location-based and remote control services. Survivor certainty is likely dependent

[51] Or non-essential functions that may otherwise have significant negative impacts for the survivor, for example complicating the survivor's ability to make timely payments.

[52] Similarly, while we urge the Commission to prioritize ease of utilization of programs and features by survivors, where this comes into conflict with survivor safety obviously safety must take priority. For example, manufacturers should be compelled to take quick action but not immediate action in response to seemingly legitimate requests that could have implications for survivor safety. Fraudulent Emergency Data Access Requests are a particularly troubling example of how these processes can be abused without adequate due diligence in place. *See, e.g.*, Comments of EPIC to the CFPB on the Required Rulemaking on Personal Financial Data Rights, at 10 (Dec. 22, 2023), https://epic.org/documents/comments-of-epic-to-the-cfpb-on-the-required-rulemaking-on-personal-financial-data-rights/#_ftnref24.

[53] FNPRM at ¶ 6, https://www.federalregister.gov/d/2024-08642/p-24. In many cases industry letters suggest this would require a court order. *See, e.g.*, Letter, Mercedes-Benz North America, WC Dkt. No. 22-238 at 2 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10227846210101; Letter, Stellantis North America, supra note 34, at 2; Letter, General Motors Company, supra note 41, at 2; Letter, Toyota Motor North America Inc., *supra* note 45 at 7.

[54] *See, e.g.*, R&O at ¶¶ 111–12.

upon providers not having to guess what obligations apply to them. The Federal Communications Commission's role is distinct from but complementary to the Federal Trade Commission's role.[55] As we discuss in sections V and VI *infra*, the Commission has ample authority to prevent these lapses as the country's watchdog for communications systems privacy and security and in its role in preserving safety of life. This is true regardless of whether provider services are offered directly or indirectly,[56] whether it is a CMRS or PMRS,[57] whether services are provided via wireline, fixed wireless or fixed satellite,[58] or whether they're mobile virtual network operators (MVNOs)[59] or voice over internet protocol (VoIP) providers.[60] The Commission should not allow for inconsistency in how the SCA protects survivors from attempts at surveillance, control, or revictimization via location-based or remote control services associated with connected cars. It would be contrary to the purpose of the SCA for there to be inconsistency in its protections based on underlying technology or based on classification of business or of usage that *from the survivor's point of view* are functionally indistinguishable from one another. The Commission should also help to resolve some of the finger-pointing evident in the industry response letters to Chairwoman Rosenworcel's inquiry, with telecom providers arguing the SCA doesn't apply here and connected car service providers arguing they aren't subject to Commission regulatory authority.[61]

The Commission should identify other relevant stakeholders in the connected car ecosystem. At a minimum these likely includes dealerships[62] and their sister finance companies or other creditors in the vehicle financing sphere who may have access to survivor data,[63] may

---

[55] While there are similarities in their consumer protection authorities, the FCC additionally has responsibility for the safety of communications infrastructure, including its implications for the personal safety of individuals. *Compare* EPIC et al. Open Internet Comments *supra* note 29, at 6, 10–12 *with* Section VI(f,g) *infra*.

[56] *See* subsection V(c) *infra*.

[57] The SCA and R&O definition of "covered provider" includes PMRS or CMRS. *See* R&O at ¶ 16; 47 C.F.R. § 64.6400(g); 47 U.S.C. § 345(a)(3).

[58] *See, e.g.*, R&O at ¶ 120.

[59] *See* subsections V(c), VI(a), VI(c) *infra*; I*n re Quadrant Holdings LLC, Q Link Wireless LLC, and Hello Mobile LLC, Notice of Apparent Liability for Forfeiture*, File No.: EB-TCD-22-00034450 at 4 n. 23 (July 28, 2023) (citing to 47 U.S.C. § 222; 47 C.F.R. § 64.2003(o); 47 U.S.C. §§ 153(51), 332(c)).

[60] *See, e.g.*, R&O at ¶ 120.

[61] *See, e.g.*, Letter, General Motors Company *supra* note 41, at 1; Letter, American Honda Motor Co., *supra* note 27, at 5; Letter, Verizon, WC Dkt. No. 22-238 at 7-8 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10227906429906.

[62] "GMC", *Privacy Not Included (review date Aug. 15, 2023), https://foundation.mozilla.org/en/privacynotincluded/gmc/ (noting GM may share data with dealers). We acknowledge that better data minimization controls by providers would likely reduce unnecessary data sharing with third parties such as dealers.

[63] *See, e.g.*, FNPRM at ¶ 13, https://www.federalregister.gov/d/2024-08642/p-31 ("Some of the responses to the information requests indicate that the provider's connected car service gives notice to a driver that the car's location is being tracked. Other responses do not indicate whether the service offers this function. The responses to the information requests further indicate that information collected through connected car services may be shared with third parties in accordance with connected car service agreements.").

manage user accounts for connected car services, or may be contacted by a survivor attempting to escape from a dangerous situation related to the vehicle. For example, in a coerced debt situation, the survivor may wish to have a vehicle voluntarily repossessed, but company policy may require the signature of the abuser as well before commencing the repossession.[64] Identifying relevant stakeholders would likely also include data brokers[65]—what types of data that brokers sell and to whom may shed additional light on vectors by which abusers might attempt to surveil, control, or re-victimize survivors.

Related to this point, the Commission should identify what other agencies the Commission may need to partner with to ensure these stakeholders comply with whatever requirements are deemed necessary to keep survivors safe.

We also urge the Commission to articulate what, if any, differences it may have in its expectations for connected car service providers as opposed to other service providers.[66] For example, are concerns about on-device data different for connected car services than for handsets or other covered devices?[67] The factual background[68] for this proceeding seems to support heightened risks associated with location data captured from a vehicle. Does the Commission weigh interests differently for vehicle tracking as they relate to survivor safety?[69] On this point, we urge the Commission to design solutions to protect survivors rather than to preemptively thwart auto theft crime rings (e.g., by requiring a police report after a theft rather than requiring a court order before requesting a line separation). The Commission has balanced equities like this in this docket before.[70]

---

[64] The National Consumer Law Center has a model law that outlines some of the contours of the coerced debt issue. *See* Andrea Bopp Stark, Carla Sanchez-Adams, National Consumer Law Center, *Model State Coerced Debt Law* (May 1, 2024), https://www.nclc.org/resources/model-state-coerced-debt-law/.

[65] *See, e.g.*, Sen. Markey Letter to Hon. Chair Lina Khan (Feb. 27, 2024), https://www.markey.senate.gov/imo/media/doc/senator_markey_letter_to_ftc_on_auto_privacy__022824pdf.pdf; "Data Brokers: What They Are and What You Can Do About Them", Safety Net Project National Network to End Domestic Violence, https://www.techsafety.org/data-brokers; Tom Kemp, How SB 362 Can Protect Domestic Violence Victims' Online Information (Updated Oct. 2023), https://www.tomkemp.ai/blog/2023/04/24/how-sb-362-can-protect-domestic-violence-victims-online-information; *see also* multiple sources cites *supra* note 30.

[66] The Commission has already done this with regards to evidentiary requirements survivors may need to satisfy in the context of connected car services. *See* FNPRM at ¶ 20, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-38 (asking "Would there be any reason to modify these evidentiary requirements for connected car services?").

[67] *See, e.g.*, R&O at ¶ 127 ("We exclude from this definition any logs of calls or text messages stored on consumers' wireless devices or wireline telephones, such as recent calls stored in the mobile device's phone app or lists of recently dialed numbers on cordless wireline handsets").

[68] *See, e.g.*, FNPRM at ¶ 1, https://www.federalregister.gov/d/2024-08642/p-19 ("news reports suggest that these services have also been used to stalk, harass, and revictimize survivors of domestic violence").

[69] *See, e.g.*, FNPRM at ¶ 24, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-42.

[70] *See, e.g.*, R&O at ¶ 76 (balancing survivor safety and needs against SIM swap fraud concerns).

IV. The Commission should define terms in alignment with the five principles, require security controls tailored to survivors, and demand transparency from private sector partners.

The Commission asks how it may better address concerns about the impact of connected car services on domestic violence survivors, including by changes to its existing rules.[71] It also asks what actions the agency can take within or outside the scope of the SCA[72] or even actions it cannot take itself but that it could encourage others to take.[73] We urge the Commission to offer definitions or interpretations of terms such as "victim services provider" that align with the five principles we outlined at the top of our comment. We also urge the Commission to require or incentivize privacy and data security controls that will help to better protect survivors, with particular sensitivity to the special concerns faced by survivors in the context of cybersecurity. While we recognize the private sector is an indispensable partner in making these changes real, we caution the Commission to demand greater transparency and employ greater skepticism in dealing with its industry partners in this effort.

a. The Commission should define "victim services provider" and other terms in a manner that aligns with our five core principles.

While we reiterate that it is damaging and counterproductive for survivors to have to prove their status as such, we recognize the Commission's established position on the matter.[74] Operating within the confines of the Safe Connections Act, survivor status can be shown by an affidavit submitted by a "victim services provider", and we further note that no license is required of that provider.[75] Moreover, neither the SCA nor the Commission's earlier Report and Order (R&O) defines the term "victim services provider." The Commission should define "victim services provider" in a manner that maximizes survivor self-determination and agency, minimizes burdens to survivors to maximize program utilization, prioritizes data minimization and data security, helps to proactively prevent misuse, and puts access burdens on providers and manufacturers rather than on survivors. This could include requiring providers processing line separation requests to accept affidavits from legal aid organizations or local members of the clergy acting as victim services providers. To avoid misuse of this process, we urge the Commission to consider when a victim services provider might be required to validate their identity as well as the authorization the survivor has given them to act on that survivor's behalf.

---

[71] *See* FNPRM at ¶ 16, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-34.

[72] *See* FNPRM at ¶ 21, https://www.federalregister.gov/d/2024-08642/p-39.

[73] *See* FNPRM at ¶ 22, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-40.

[74] *See* R&O at ¶ 31.

[75] *See* Safe Connections Act of 2022, H.R. 7132, 117th Cong. § 4(c)(1)(A)(i) (2022), https://www.congress.gov/bill/117th-congress/house-bill/7132/text ("a copy of a signed affidavit from a *licensed* medical or mental health care provider, *licensed* military medical or mental health care provider, *licensed* social worker, *victim services provider*, or *licensed* military victim services provider") (emphasis added) [hereinafter "SCA"]; 47 C.F.R. § 64.6401(a)(9)(i); R&O at ¶ 36.

The Commission should also explicitly state that identity theft reports[76] filed with the Federal Trade Commission constitute acceptable documentation of survivor status, as that is a report filed with a law enforcement agency.

b. The Commission should require or incentivize privacy and data security controls that protect survivors, being mindful of special privacy and cybersecurity concerns faced by survivors.

Survivors face situations that are counterintuitive to many conventional assumptions in cybersecurity and may more nearly approximate insider threat concerns. For example, the threat actor likely has physical access to the survivor's device and likely knows or can acquire the answers to their security questions. Further complicating the matter, the abuser may have given themselves administrative privileges and assigned the survivor a user account with diminished privileges subject to abuser monitoring or control.[77] Or the abuser may have installed stalkerware that tracks web browsing activity, logs keystrokes, or captures video recording of the survivor's device activity. While the Commission cannot solve for all of these problems, it can consider workable solutions. For example, the Commission could require that the portal for line separation requests be used for a variety of innocuous purposes so that if an abuser learns a survivor accessed the portal, the survivor will not necessarily be exposed to enhanced risk of retaliation.

Products should be designed to support any intended victim—for example, alerting them to monitoring and allowing them to disable monitoring in a readily-transparent and -accessible manner. As we discuss in the context of consent above, subsections II(c) and II(d) *supra*, these alerts should not occur only once, nor at a predictable interval. Unfortunately, industry response letters suggest standard practice may not align with these design principles.[78] An audit log of user access to vehicle location data could be a useful design feature. In terms of process, disabling monitoring should not require something so labor-intensive as obtaining a court order. On the flip side, in terms of obtaining increased access to data, in some instances it may be appropriate to require a police report be filed before location data can be turned over to another user. Because law enforcement may side with an abuser rather than their victim,[79] a subpoena should be required for law enforcement access to location data, not a mere informal request.

c. The Commission should demand greater transparency from and employ greater skepticism when dealing with its private sector partners.

Mobility data is extremely desirable. As the Future of Privacy Forum and Mobility Data Collaborative noted: "[t]he sensitivity of mobility data may make it a particularly attractive target for criminals, malicious actors, and other prying eyes, including employees who may try to

---

[76] For example, in the case of coerced debt. *See* "Coerced Debt," *supra* note 46.

[77] *Compare* EPIC et al. Reply Comments at 5 *with* Ruiz, *supra* note 41 ("Because the separate woman was a "primary" account owner, she was able to remove the car's access to the internet, Reuters reported.").

[78] Letter, Verizon, *supra* note 61, at 9 ("Hum account owners can share vehicle location with family members on their Hum account at their election.").

[79] *See* R&O at ¶ 38; EPIC NNEDV et al. NPRM Comments at 13, App'x 2, PDF pgs 39-40/40.

exceed their authorized use for personal gain."[80] And this does not speak to business or other financial incentives to collect and share location data and other vehicle data.[81]

While it is easy to see the extent to which carriers' actions continue to be deficient in the context of robocalls and SIM swapping, it can be harder to detect and demonstrate impacts on marginalized and vulnerable populations such as survivors of domestic violence. As such, the Commission should apply additional scrutiny to providers' claims of effective efforts to support survivors.

The connected car services industry is no different, and may be worse. One need only compare their promotion of their privacy principles against Mozilla reporting and security researcher vulnerability disclosures.[82] Additionally, many automakers did not offer clarification about what services are opted into by default in response to Sen. Markey's 2023 letters to the industry.[83] It is not surprising that at least one company seems to have given conflicting information to the Commission and to Mozilla regarding the sale of data to third parties for marketing purposes.[84] Another response letter to Chairwoman Rosenworcel notes that they were not the proper entity to receive the Commission's inquiry.[85]

V. The Commission has authority for its proposed regulations under the Safe Connections Act.

a. The SCA empowers the Commission to regulate line separations regardless of underlying technology used or of classification of services provided

Regardless of underlying technology used to provide the mobile service, and regardless of classification of services provided (e.g., voice, text, or data), the Commission has established that the SCA's line separation provisions apply.

---

[80] *Mobility Data Sharing Assessment: Operator's Manual*, 32 (Aug. 2021), https://fpf.org/wp-content/uploads/2021/08/2-MDSA-Operators-Manual.pdf; *see also* EPIC NNEDV et al. NPRM Comments at App'x 2.

[81] *See, e.g.*, Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies*, New York Times (updated Mar. 13, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html; Justin Sherman, *People Search Data Brokers, Stalking, and 'Publically Available Information' Carve-Outs*, Lawfare (Oct. 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs.

[82] Section II(c) *supra.*

[83] *See* Senator Markey Letters to Automakers on Privacy (Nov. 30, 2023), https://www.markey.senate.gov/imo/media/doc/senator_markey_letter_to_automakers_on_privacy.pdf.

[84] *See* Letter, American Honda Motor Co., *supra* note 27; "Honda", *Privacy Not Included), *supra* note 27.

[85] *See* Letter, Hyundai Motor America, *supra* note 26.

The SCA explicitly states that the term "covered provider" includes a provider of a private mobile service as well as a provider of a commercial mobile service.[86] In promulgating its implementing regulations, the Commission made it clear that line separation obligations apply to all providers of commercial mobile service or private mobile service, "as the Commission might interpret and apply those definitions, *regardless of the underlying technology used to provide the service*."[87] (emphasis added). As one example, we note that the Commission has already found Onstar to be a commercial mobile service provider (although the FCC noted at the time that not all of Onstar's units were capable of wireless calling).[88] We also note that the Commission recently reinstated its classification of mobile broadband internet access service as a commercial mobile service.[89]

Similarly, the Commission has defined a "line of service" as including "all of the services associated with that line under the shared mobile service contract, regardless of classification, including voice, text, and data services."[90] In its Report and Order, the Commission implied that even if a device lacked voice service or capabilities over commercial mobile radio service, a survivor should still be able to use it with over-the-top (OTT) services to send and receive messages or make voice calls using data or data messaging services without fear of being monitored by an abuser.[91] Indeed, even if a device only nominally has a line associated with a customer, such as a tablet with no mobile capability, it could still be a vector by which an abuser attempts to exert control and from which a survivor should be able to separate themself per Congress' directive through the Safe Connections Act.[92] As such, even if all phone calls and text

[86] 47 U.S.C. § 345(a)(3) ("as those terms are defined in section 332(d)"). *See also* 47 C.F.R. § 64.6400(g); R&O at ¶ 16.

[87] R&O at ¶ 16.

[88] *See* Report and Order, In re Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems, CC Docket No. 94-102 at ¶ 18 (Rel. Oct. 21, 2003), https://docs.fcc.gov/public/attachments/FCC-03-242A1.pdf ("although OnStar telematics units do not have the appearance of "traditional" portable handsets, we find that some units are also capable of providing a commercial mobile radio service (CMRS) in addition to telematics services. 911 calls may be made from them over the underlying CMRS network of the carrier licensees, with whom OnStar has reached agreements to provide that wireless service, and thus may be potentially used by the licensee to determine the location of those calls. We do not agree with the contention in some comments that because the CMRS offered by OnStar is optional, ancillary, or tethered, those OnStar telematics units are not within the scope of Part 20. Their capability to function as mobile phones within the general definitions we have considered and to provide commercial wireless service through a licensee qualifies them as mobile phones within the definition Section 20.3…") (internal citations omitted).

[89] *See* Declaratory Ruling, Order, Report and Order, and Order on Reconsideration, In re Safeguarding and Securing the Open Internet, Restoring Internet Freedom, WC Dkt. Nos. 23-320, 17-108 at ¶ 6, 25, 214 (Rel. May 7, 2024), https://docs.fcc.gov/public/attachments/FCC-24-52A1.pdf [hereinafter "Open Internet Order"].

[90] 47 C.F.R. § 64.6400(k).

[91] *See* R&O at at ¶ 20.

[92] *See id.* at ¶ 21.

messages to and from a given number are blocked on a device,[93] that device is not necessarily beyond the scope of the SCA.

b. The SCA empowers the Commission to interpret its implementing regulations broadly to reduce survivor uncertainty due to functionally indistinguishable technical classifications.

The SCA also empowers the Commission to apply a similar rationale as it applied to its call log regulations to its regulation of location-based and remote control services that could be used by an abuser to attempt to surveil, control, or revictimize[94]—namely, reducing survivor uncertainty caused by functionally indistinguishable technical classifications.

To fulfill the statutory goals of the SCA, the Commission extended its call log rules to voice service providers beyond the Act's definition of "covered providers", noting that a survivor "often would not appreciate the legal nicety" that the Commission's rules shielded only certain types of calls but not others that, from the survivor's point of view, were functionally indistinguishable.[95] The Commission found that failing to apply the rule to all providers would create uncertainty that would undermine the Act's overall goal of establishing "safeguards within communications services [that] can serve a role in preventing abuse."[96]

The SCA is designed to put survivors first. It retained the definition of "voice service" from the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act.[97] In its Report and Order, the Commission explicitly noted that this definition includes transmissions from computers and services that permit outbound calling, regardless of whether it is one-way or two-way voice over internet protocol (VoIP) service, and applies to wireline, fixed wireless, and fixed satellite providers of voice service.[98] Additionally, the Commission's definitions for voice service providers were explicitly not limited to retail service.[99]

Similarly, the Commission should not allow for inconsistency in how the SCA protects survivors from attempts at surveillance, control, or revictimization via location-based or remote control services. It would be contrary to the purpose of the SCA for there to be inconsistency in its protections based on underlying technology or based on classification of business or of usage if *from the survivor's point of view* these classifications are functionally indistinguishable from one another. As with its call log rule, to allow for such uncertainty would undermine the Act's goal to establish safeguards to prevent abuse within communications services.

---

[93] *See, e.g.*, Letter, Ford Motor Company, *supra* note 41, at 1.

[94] FNPRM at ¶ 12, https://www.federalregister.gov/d/2024-08642/p-30.

[95] R&O at ¶ 111.

[96] R&O at ¶ 112.

[97] *See* SCA § 5(a)(8); 47 C.F.R. § 64.6400(o).

[98] *See, e.g.*, R&O at ¶ 120.

[99] *See, e.g.*, R&O at ¶ 114. The SCA exempts enterprise services from its definition of "shared mobile service contract." 47 U.S.C. § 345 (a)(5)(B).

Absent a consistent, visible notification that the car's location can be accessed (accessed either in real-time or in the future), the survivor may believe that they are travelling safely. Like an abuser seeing a call to a hotline or shelter in a customer-facing call log, an abuser seeing a record of a visit to a victim service organization captured by a car's location-based services could result in increased risk to the survivor, unbeknownst to the survivor.

We offer further sources of the authority the Commission might draw upon in Section VI, *infra*, but we reiterate that the SCA already gives the FCC authority to resolve this risk of survivor uncertainty.

c. Service providers cannot evade all SCA obligations by claiming an indirect relationship to their survivor-customer.

Whether the relationship between the provider and the survivor is direct or indirect[100] also should not matter, especially not in an analysis from the survivor's perspective. It may impact which responsibilities each entity has for fulfilling the obligations of the Act and of the Act's implementing regulations, however. The Commission addressed the relationship between mobile virtual network operators (MVNOs) and their underlying providers in its Report and Order, noting that to the "extent an MVNO controls any facilities or systems (for example, customer care or billing), the obligations imposed by the SCA fall entirely on the MVNO and not the underlying facilities-based provider."[101]

As relates to call logs, an underlying facilities-based provider that produces call logs that are consumer-facing towards the wholesale customers' end user customers is obligated to comply with the Commission's rules, and resellers who do not control their own call logs are expected "to make good faith efforts, such as through their contracts, to ensure that their wholesale providers are complying" with the FCC's rules.[102] Similarly, it would undermine the Act's goal of securing communications services against misuse by abusers if both resellers and their partners were beyond the Commission's authority.

The SCA authorizes the Commission to require resellers who do not control the location-based or remote control services they offer to end user consumers (e.g., survivors) to make good faith efforts—such as through their contracts—to ensure that wholesaler business partners responsible for location-based or remote control services are abiding by the Commission's SCA regulations.

VI. The Commission has authority beyond the Safe Connections Act.

Whether or not the Commission chooses to rely on the SCA, other provisions of the Communications Act provide ample authority to support the assertion of its authority to protect survivors from attempted surveillance, control, and revictimization by an abuser by regulating location-based and remote access services in connected cars. These authorities include but are not limited to regulating cars to the extent that they are mobile virtual network operators

[100] *See* FNPRM at ¶ 11, https://www.federalregister.gov/d/2024-08642/p-29.

[101] R&O at ¶ 17.

[102] R&O at ¶ 114.

(MVNOs) or to the extent that cars connect to the public switched network. For example, even outside of the SCA, to the extent the Commission finds that automobile manufacturers are MVNOs or provide CMRS service directly by interconnecting with the Public Switched Network (PSN), the Commission's general Title II powers apply.[103] Because connected car services involve the use of wireless, the Commission may regulate its use pursuant to the Commission's Title III authorities and Section 705.[104] Finally, its general authority over the privacy and cybersecurity of communications networks, and its mandate to protect safety of life through use of communications systems, provide the Commission with both direct and ancillary authority to adopt rules.[105]

a. MVNOs

A mobile virtual network operator (MVNO) is a reseller of mobile service. MVNOs are not facilities-based providers but rather resell access to the networks of facilities-based providers.[106] For example, as of 2021, TracFone was the largest MVNO,[107] reselling access to networks including AT&T, T-Mobile, and US Cellular.[108] From their inception, MVNOs were differentiated as a type of reseller that by virtue of their brand development have greater control over subscribers and better penetration into niche markets than a national company concerned with large market segments.[109] Based on their responses to Chairwoman Rosenworcel's letters, many car companies seem not to be facilities-based providers but rather to resell access to the networks of a facilities-based provider, making them an MVNO.[110] Similarly, many telecom providers in their responses to Chairwoman Rosenworcel's letters noted that they merely sold bandwidth to car companies, that they had no visibility into end user consumers or data usage, and that they could not comply with the Commission's proposed regulations because the end user survivors were not their customers (although we do not concede that a company is exempt

[103] *See, e.g.*, 47 U.S.C. §§ 201(b), 222(a), 222(c), 251(e).

[104] Indeed, the Commission has used its general authority to regulate the use of spectrum in the public interest (whether on a licensed or unlicensed basis) to prohibit the use of eavesdropping devices since 1966. *See* 43 FR 3397 (adopting Rules 2.701 and 15.11).

[105] *See* 47 U.S.C. §§ 151, 154(i), 154(n), 606.

[106] *See, e.g.*, Memorandum Opinion and Order, *In re Application of Verizon Communications Inc.*, GN Docket No. 21-112 at 13 n. 88 (Nov. 22, 2021), https://docs.fcc.gov/public/attachments/FCC-21-121A1.pdf ("MVNOs do not own any network facilities, but instead purchase mobile wireless services wholesale from facilities-based service providers and resell these services") (citing to 2020 Communications Marketplace Report, 36 FCC Rcd at 2951, para. 12).

[107] *Id*. at ¶ 34.

[108] *Id*. at ¶ 113.

[109] *See* Seventh Report, *In re Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions With Respect to Commercial Mobile Services*, 17 FCC Rcd 12985, 13025 (Rel. July 3, 2002), https://docs.fcc.gov/public/attachments/FCC-02-179A1.pdf PDF pg 41/145.

[110] *See, e.g.*, Letter, Stellantis North America, *supra* note 34, at 1; Letter, General Motors Company, *supra* note 41, at 2; Letter, Nissan North America, Inc., *supra* note 34, at 2; Letter, Ford Motor Company *supra* note 41, at 2.

from Commission authority merely because those who rely upon its service are not its customers).[111]

Based on both car and telecom company responses to Chairwoman Rosenworcel's letters, car companies are likely MVNOs. As described above, in Section V *supra*, MVNOs are responsible for complying with the SCA to the extent that they control any facilities or systems (e.g., customer care, billing, etc.).[112] Additionally, resellers are expected "to make good faith efforts, such as through their contracts, to ensure that their wholesale providers are complying" with the FCC's rules.[113]

b. Public Switched Network

To the extent that a connected car company's offerings use North American Numbering Plan (NANP) resources in connection with the provision of switched services, they are CMRS and therefore covered by Title II.[114] To the extent that these offerings include broadband services, they will imminently be subject to FCC regulatory authority.[115] We note that nongeographic numbers are still NANP numbers.[116] Additionally, the Commission has established its authority over the "public switched network," not merely the "public switched telephone network."[117] This includes "any common carrier switched network, whether by wire or by radio . . . that use[s] the North American Numbering Plan, or public IP addresses, in connection with the provision of switched services."[118] To the extent that connected cars use NANP or public IP addresses in connection with the provision of switched services, the Commission has regulatory authority.

---

[111] *See, e.g.*, Letter, Verizon *supra* note 61, at 4; Letter, AT&T Services Inc., WC Dkt. No. 22-238 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1022780536850; Letter, T-Mobile USA, Inc., WC Dkt. No. 22-238 at 2-3 (Feb. 27, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/102271531023780.

[112] *See* FNPRM at ¶ 18, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-36.

[113] R&O at ¶ 114.

[114] 47 U.S.C. § 332(d).

[115] To the extent a finding of interconnection with the PSN depends on the reclassification of broadband as a Title II service, and the expanded definition of PSN adopted in the Open Internet Order, it will take effect 60 days after publication in the federal register. *See* Open Internet Order at ¶ 710. Publication occurred on May 22, 2024. Final Rule, *Safeguarding and Securing the Open Internet; Restoring Internet Freedom*, 89 FR 45404 (May 22, 2024), https://www.federalregister.gov/documents/2024/05/22/2024-10674/safeguarding-and-securing-the-open-internet-restoring-internet-freedom.

[116] *See, e.g.*, "NPA (Area Codes)", NANPA, https://nationalnanpa.com/area_codes/ ("These reports include identification of geographic area codes (i.e., area codes that designate specific geographic areas) and non-geographic area codes"); Letter, Verizon, *supra* note 61, at 7–8 ("Even to the extent that a billed line for a Hum or Connected Car Wi-Fi subscriber arguably falls within the scope of the definition, it is not technically feasible to include a non-geographic number as part of a line separation request").

[117] Open Internet Order at ¶¶ 219–25.

[118] *Id.* at ¶ 219 n. 922 (citing to 2023 Open Internet NPRM at 47, ¶ 87; 2015 Open Internet Order, 30 FCC Rcd at 5779, ¶ 391).

We ask the Commission to clarify that providers who are subject to any one relevant Commission authority are subject to the Commission's proposed rule even if they may not be subject to other listed authorities. This may be helpful because the Commission has said that a telematics unit that can only transmit voice and data communications to the telematics call center does not use the interconnected public switched network.[119] However, such an entity is still subject to other relevant Commission authorities, such as the Commission's numbering authority (see immediately below). Alternatively, we ask the Commission to revisit whether devices and services utilized for the purposes of emergency communications are subject to the Commission's regulatory authority over the public switched network even if those devices or services only readily connect to a portion of rather than to the entirety of the public switched network.

c. Title II authorities (201(b), CPNI, and numbering)

A shell game cannot frustrate the Commission's Title II regulatory authority. Whichever entity acts as carrier or under direction of a carrier (including as designee of the carrier) is subject to the Commission's Title II authority.[120] If the car connects to the PSN, then Title II applies. Nor is this a determination left to the car companies or the carriers, but a legal conclusion for the Commission to determine. Accordingly, Hyundai's statement that a different subsidiary than the one responding to Chairwoman Rosenworcel's letter acts as an MVNO,[121] or the assertion of other car companies that 'we are not an MVNO,' is of no moment. The Commission should be clear that this does not excuse the responsible party from its obligations under the SCA (and other applicable authorities) to prevent misuses of the communications network that perpetrate domestic violence.

As we argue in our reply comments and above,[122] survivors often did not 'assume the risk' as they did not install or request the services being used to surveil or control them,[123] and saying that a survivor assumes the risk every time they enter a connected car would be forcing them to choose between personal transportation and personal safety[124] and put them into

[119] *See* Report and Order, *In re Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102 at ¶ 17 (Rel. Oct. 21, 2003), https://docs.fcc.gov/public/attachments/FCC-03-242A1.pdf.

[120] *See* Declaratory Ruling, *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115 at ¶ 23 (Rel. June 27, 2013), https://docs.fcc.gov/public/attachments/FCC-13-89A1.pdf ("We also conclude that information that a carrier causes to be stored on its customer's device in order to allow the information to be shared with the carrier is 'made available to the carrier by the customer solely by virtue of the carrier-customer relationship.' This is true whether the carrier itself installs, or directs the installation of, the software that collects the information, and whether the information is shared directly with the carrier or with its designee.").

[121] *See* Letter, Hyundai Motor America, *supra* note 26.

[122] *See* subsection II(c) *supra*.

[123] *See* EPIC et al. Reply Comments at 6 n 24.

[124] *See, e.g.,* FNPRM at ¶ 2, https://www.federalregister.gov/d/2024-08642/p-20 ("We seek comment on solutions to help ensure that domestic violence survivors need not choose between access to personal transportation or exposing themselves to threatening, stalking, or other harmful behavior by those who

uncertainty about when the Commission's protections applied to them, undermining the goals of the SCA[125] and of the public interest.

1. Section 201(b)

Section 201(b)[126] prohibits a Title II carrier from engaging in unjust and reasonable practices. As the Commission has previously found, Section 201(b) provides the Commission with broad consumer protection authority—including the power to impose rules protecting privacy.[127] Even if the Commission concludes that the SCA does not universally apply, the Commission may adopt necessary rules pursuant to its Section 201(b) authority. The findings made by Congress in Section 3 of the SCA support the conclusion that failure to take action to protect domestic abuse survivors would be unjust, unreasonable, and contrary to the public interest.

2. Section 222

Customer proprietary network information (CPNI) rules safeguard subscriber privacy[128] collected by or on behalf of telecommunications providers, which include MVNOs[129] and interconnected VoIP providers.[130] As we have noted in several dockets, the Commission has

---

can access the car's data and connectivity."); Statement of Chairwoman Jessica Rosenworcel, *National Plan to End Gender-Based Violence One Year Anniversary* at 2 (May 15, 2024), https://docs.fcc.gov/public/attachments/DOC-402577A1.pdf ("The bottom line is that no survivor of domestic violence and abuse should have to choose between giving up their vehicle and allowing themselves to be stalked and harmed by those who can access its connections and sensitive data about where they go and what they do."); Statement of Chairwoman Jessica Rosenworcel, Further Notice of Proposed Rulemaking, *In re Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238 (Apr. 8, 2024), https://docs.fcc.gov/public/attachments/FCC-24-38A2.pdf ("No survivor of domestic violence and abuse should have to choose between giving up their car and allowing themselves to be stalked and harmed by those who can access its connectivity and data.").

[125] *See, e.g.*, subsections II(e), V(b) *supra*.

[126] 47 U.S.C. § 201(b).

[127] *See, e.g.*, Fed. Commc'ns Comm'n, *In re Data Breach Reporting Requirements*, Report and Order, FCC 23-111 at ¶ 126 (Rel. Dec. 21, 2023), https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf (finding it to be "implausible that Congress would have exempted common carriers from any obligation to protect their customers' private information that is not CPNI" in the context of its data privacy and data protection authority under Section 201(b)); Reply Comments of EPIC, Center for Democracy and Technology, Privacy Rights Clearinghouse, and Public Knowledge, *In re Data Breach Reporting Requirements*, WC Docket No. 22-21 at 9-11 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814 [hereinafter "EPIC et al. Data Breach Reporting Requirements Reply Comments"]; EPIC et al. Open Internet Comments at 10-12; Reply Comments of EPIC at al., *In re Protecting Consumers from SIM-Swap and Port-Out Fraud*, WC Dkt. No. 21-341 at 3-7 (Feb. 12, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10213160552872.

[128] *See, e.g.*, 47 C.F.R. §§ 64.2001-64.2011.

[129] *See, e.g.*, In re *Quadrant Holdings LLC*, et al. *supra* note 59 (Section 222 and CPNI Rule enforcement action against two companies that were common carriers and MVNOs).

[130] *See, e.g.*, Pretexting Order at ¶ 1 n. 3.

established through its rules and its enforcement that CPNI includes device location data.[131] Even if the CPNI has not yet been transferred to the carrier, if the carrier is able to access it and the CPNI was collected at the carrier's direction or by the carrier's design, it is protected.[132]

Furthermore, the Commission has repeatedly found that Section 222(a) imposes a general obligation on carriers to protect the proprietary information of customers. As the Commission concluded when protecting victims from stalkers in 2007 in the CPNI Pretexting Order: "CPNI includes personally identifying information."[133] This authority includes the power to require telecommunications providers to implement procedures and safeguards that prevent unauthorized access to personally identifying information,[134] particularly where disclosure of the information would jeopardize an individual's safety.[135] Even in situations where the SCA does not apply, the Commission may adopt necessary regulations pursuant to its authority under Section 222.

3. Section 251(e)

Under Title II the Commission also has "exclusive jurisdiction over those portions of the North American Numbering Plan that pertain to the United States."[136] As noted above, NANP numbers include both geographic and non-geographic numbers. To the extent that connected cars

[131] *See, e.g.*, Press Release, *FCC Fines AT&T, Sprint, T-Mobile, and Verizon Nearly $200 Million for Illegally Sharing Access to Customers' Location Data* (Apr. 29, 2024), https://www.fcc.gov/document/fcc-fines-largest-wireless-carriers-sharing-location-data; Report and Order, *In re Location-Based Routing for Wireless 911 Calls*, PS Dkt. No. 18-64 at ¶ 103 (Jan. 26, 2024), https://docs.fcc.gov/public/attachments/FCC-24-4A1.pdf ("EPIC also asks the Commission to clarify how its privacy and security rules, including those governing using, disclosing, and permitting access to Customer Proprietary Network Information (CPNI), apply to device-based location data. Section 222 of the Communications Act of 1934, as amended, requires CMRS providers, among others, to protect the confidentiality of location information and prohibits them from using, disclosing, or permitting access to location information without the customer's express prior authorization…") (internal citations omitted); EPIC et al. Open Internet Comments at 8-9; Comments of EPIC, *In re Protecting Consumers from SIM-Swap and Port-Out Fraud*, WC Dkt. No. 21-341 at 8 (Jan. 16, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1011728090306.

[132] *See* Declaratory Ruling, *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115 at ¶ 27 (Rel. June 27, 2013), https://docs.fcc.gov/public/attachments/FCC-13-89A1.pdf ("CPNI is defined as information that is *made available to the carrier;* even if that information has not yet been transmitted from the mobile device to the carrier, the configuration of the device has made the information available to carrier.") (emphasis original).

[133] Pretexting Order at ¶ 4 n.6.

[134] *See, e.g.*, EPIC et al. Open Internet Comments at 9; EPIC et al. Data Breach Reporting Requirements Reply Comments at 5-8.

[135] *See, e.g.*, Pretexting Order at ¶ 58 ("If we failed to exercise our responsibilities under sections 222 and 1 of the Act with respect to customers of interconnected VoIP service, a significant number of American consumers might suffer a loss of privacy and/or safety resulting from unauthorized disclosure of their CPNI -- and be harmed by this loss.").

[136] 47 U.S.C. § 251(e).

utilize NANP numbers allocated to the United States, the Commission has exclusive jurisdiction over their use of those numbers; this jurisdiction includes regulatory authority.[137]

The Commission has previously concluded that it may condition assignment of phone numbers on requirements to protect the privacy of subscribers.[138] As the Commission observed in its recent Order on SIM swap and port-out fraud: "Congress expressly assigned to the Commission exclusive jurisdiction over that portion of the NANP that pertains to the United States and related telephone numbering issues. The Commission retained its authority to set policy with respect to all facets of numbering administration in the United States."[139]

d. Title III authorities

Regardless of whether a car company is determined to be an MVNO, the provision of WiFi within the vehicle subjects the company to the Commission's Title III authority. This is true both in the general context of wireless communications as a sector[140] and in the specific context of prohibiting the interception or disclosure of wireless communications.

As early as 1966, the Commission exercised its Title III authority to prohibit the use of any wireless device—whether using licensed or unlicensed spectrum—to listen to the conversation of others without consent.[141] While the Commission made passing reference to various provisions of the Act, the Commission relied primarily on its general public interest authority pursuant to Sections 301, 303(b) and 303(r).[142] As the Commission observed when adopting the rules: "the right of privacy is precious."[143] This is even more true here, where safety of life is involved.

e. Section 705 (47 U.S.C. § 605(a))

Section 705 is older than the Communications Act, being descended from Section 27 of the Federal Radio Act of 1927.[144] As the provision clearly states, it applies to *any* "person

---

[137] *See, e.g.*, New York v. FCC, 267 F.3d 91 (2nd Cir. 2001).

[138] *See, e.g.*, *In re Data Breach Reporting Requirements*, Report & Order, WC Docket No. 22-21 at ¶ 129, (Rel. Dec. 21, 2023); *In re Protecting Consumers from SIM Swap and Port-Out Fraud*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 21-341 at ¶¶ 92-94 (rel. Nov. 16, 2023) [hereinafter "SIM Swap Order"].

[139] SIM Swap Order at ¶ 94.

[140] Title III affords the Commission "broad authority to manage spectrum…in the public interest." *See, e.g.*, Cellco Partn. v. F.C.C., 700 F.3d 534, 541 (quoting *Data Roaming Order*, 26 F.C.C.R. at 5440 ¶ 62). This includes "mak[ing] rules and regulations and prescribing restrictions and conditions" as may be necessary to execute its authority over spectrum. *See id.* at 542 (citing to *Data Roaming Order* at 5440 ¶ 62, quoting 47 U.S.C. § 303). The Commission also explicitly has the authority to modify existing licenses if it determines such action "will promote the public interest, convenience, and necessity." *Id.* at 542 (citing to *Data Roaming Order* at 5441 ¶ 62, which quotes 47 U.S.C. § 316 and cites *Celtronix Telemetry v. FCC*, 272 F.3d 585, 589 (D.C.Cir.2001)).

[141] *See In re Prohibiting Use of Radio Devices for Eavesdropping*, 31 Fed. Reg. 3397-3400 (1966).

[142] *See id.* at 3399-40.

[143] *Id.* at 3398.

[144] Pub L. 69-632.

receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio."[145] This sweeping language clearly encompasses car manufacturers that collect personal information.

As we noted in our reply comments, the Commission has investigated the collection of data over WiFi—including location data—as a potential violation of Section 705(a) of the Communications Act.[146] In terms of how the Commission might adapt this authority,[147] the Commission could prohibit disclosure to an alleged abuser, even if the alleged abuser would otherwise be an authorized recipient of the location data.

f. Privacy and Cybersecurity

In addition to these specific provisions, the Federal Communications Commission is generally charged with ensuring the safe, secure functioning of our nation's communications infrastructure, including the privacy of the data collected as part of those communications.[148] While the Federal Trade Commission can bring enforcement actions against individual companies, it is difficult for that agency to enact new regulations.[149] It falls to the FCC to be the more nimble regulator in adapting to new threats to our communications infrastructure and to the privacy of the data transmitted across it, especially in the absence of a comprehensive federal privacy law. Additionally, the Commission's cybersecurity equities are not limited to concerns of national security but also pertain to personal safety.

g. Safety of Life

The Commission was established in part "for the purpose of promoting safety of life and property through use of wire and radio communications."[150] As the Commission has already noted in its Report and Order: "Domestic violence remains a significant safety and public health issue that results in individual harm and societal costs, affecting not just survivors but also their

---

[145] 47 U.S.C. § 605(a).

[146] *See, e.g.*, EPIC et al. Reply Comments at 9 n 35 (citing to *In re* Google, Inc., EB-10-IH-4055, DA 12-592, Notice of Apparent Liability for Forfeiture at ¶ 3 (Apr. 13, 2012), https://transition.fcc.gov/DA-12-592A1.pdf; 47 U.S.C. § 605).

[147] *See* FNPRM at ¶ 21,https://www.federalregister.gov/d/2024-08642/p-39.

[148] *See, e.g.*, "Protecting Your Personal Data", Fed. Commc'ns Comm'n, https://www.fcc.gov/protecting-your-personal-data; "Privacy/Data Security/Cybersecurity: Customer Proprietary Network Information", Fed. Commc'ns Comm'n, https://www.fcc.gov/enforcement/areas/privacy ; "Privacy and Data Protection Task Force", Fed. Commc'ns Comm'n, https://www.fcc.gov/privacy-and-data-protection-task-force ("The FCC has an important role to play ensuring the privacy of consumer communications").

[149] *See, e.g.*, Fed. Trade Comm'n, Advaned Notice of Proposed Rulemaking (ANPR), *Trade Regulation Rule on Commercial Surveillance and Data Security*, 87 Fed. Reg. 51,273 (advanced notice issued Aug. 22, 2022), https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security (2022 ANPR on data security and commercial surveillance following more than a decade of individual enforcement actions). As of the time of this writing, this FTC's ANPR has not yet progressed into an NPRM.

[150] 47 U.S.C. § 151.

families, friends, and colleagues."[151] The Commission also cited to Congress's explicit findings in the SCA, namely 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."[152] Taken together, this suggests that the Commission's directives to promote "safety of life" and to consider the public interest in regulating our nation's communications infrastructure demand that it use its authority to prevent the misuse of that infrastructure to perpetrate domestic violence.[153]

The above list of authorities is not meant to be comprehensive or dispositive; the Commission has already listed several other legal bases for its SCA-related actions.[154]

VII. Conclusion

We appreciate the opportunity to file reply comments to the Commission's FNPRM on supporting survivors of domestic violence.

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

Harold Feld
Senior Vice President
Public Knowledge
1818 N Street, NW, Suite 410
Washington, DC 20036

[151] R&O at ¶ 2; re-iterated in this FNPRM at ¶ 3, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-21.

[152] FNPRM at ¶ 4, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-22 (citing to SCA § 3(3), § 3(4)).

[153] This could include but is not limited to mandatory data collection as part of an investigation or study on promoting safety of life. *See* 47 U.S.C. § 154(n).

[154] *See* FNPRM at ¶ 28, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-46; R&O at ¶ 188.