Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
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
	)	

REPLY COMMENTS ON NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC),
Clinic to End Tech Abuse (CETA),
National Network to End Domestic Violence (NNEDV),
Public Knowledge, and
Communications Workers of America (CWA),
Cyber Civil Rights Initiative (CCRI),
Electronic Frontier Foundation (EFF),
Iowa Coalition Against Domestic Violence (ICADV),
National Coalition Against Domestic Violence (NCADV),
The National Consumer Law Center, on behalf of its low-income clients,
The National Domestic Violence Hotline,
Ohio Domestic Violence Network (ODVN),
Pennsylvania Coalition Against Domestic Violence (PCADV),
The Pennsylvania Utility Law Project (PULP),
Thomas Kadri (Assistant Prof. Law, U. Ga. School of Law)

Submitted May 12, 2023

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

Erica Olsen, Safety Net Senior Director
National Network to End Domestic Violence
1325 Massachusetts Ave NW, 7th Floor
Washington, DC 20005-4188

Lana Ramjit, Dir. Operations
Clinic to End Tech Abuse
2 West Loop Rd
New York, NY 10044

Nick Garcia, Policy Counsel
Public Knowledge
1818 N St, Suite 410
Washington, DC 20036

Summary

Electronic Privacy Information Center (EPIC), Clinic to End Tech Abuse (CETA), National Network to End Domestic Violence (NNEDV), Public Knowledge, Communications Workers of America (CWA), Cyber Civil Rights Initiative (CCRI), Electronic Frontier Foundation (EFF), Iowa Coalition Against Domestic Violence (ICADV), National Coalition Against Domestic Violence (NCADV), The National Consumer Law Center (NCLC), on behalf of its low-income clients, The National Domestic Violence Hotline, Ohio Domestic Violence Network (ODVN), Pennsylvania Coalition Against Domestic Violence (PCADV), The Pennsylvania Utility Law Project (PULP), and Thomas Kadri (Assistant Prof. Law, U. Ga. School of Law) ("Survivor Advocates") file these reply comments to recognize the support in the record for survivor self-certification and a presumption of financial hardship (Section II), to acknowledge the potential opportunities and unintended consequences of the proposals Survivor Advocates and others have supported (Section III), and to build a more robust record regarding the privacy concerns facing survivors of domestic and sexual violence (Section IV).

Table of Contents

Summary

I. Introduction **1**

II. The Record Supports Our Comments on Eligibility. **1**

III. The Commission Should Consider a Discounted Device Program, No Inactivity-Triggered De-activation of Benefits, and Certain Logistical Challenges of Line Separation. **3**

IV. The Commission Should Address Additional Privacy Concerns. **5**

a. The Commission Should Investigate Family Tracker Apps and Similar Apps 5

b. The Commission Should Articulate a Preliminary List of Its Legal Authorities to Protect Survivor CPNI from Products and Services That Are Strictly Stalkerware 8

c. The Commission Should Require Carriers to Protect Survivor Data from Unauthorized Access by Law Enforcement or by Their Own Employees 9

d. It Is Inappropriate to Flag 911 Calls as Coming from a Separated Line 10

V. Conclusion **11**

Comments

I. Introduction

The **Electronic Privacy Information Center (EPIC), the Clinic to End Tech Abuse (CETA), the National Network to End Domestic Violence (NNEDV), Public Knowledge,** and the undersigned survivor advocacy and direct service organizations ("Survivor Advocates")[1] submit these reply comments to the Federal Communications Commission (FCC, or "Commission") regarding supporting survivors of domestic and sexual violence (hereinafter "domestic violence") through its implementation of the Safe Connections Act.[2]

We file these reply comments to emphasize that: other comments in this rulemaking have provided additional support for our initial comments on eligibility; there are important points raised about discounted devices, non-usage termination, and the logistics of line separation; and there are additional privacy concerns the Commission should address in this rulemaking.

II. The Record Supports Our Comments on Eligibility.

Throughout this rulemaking, Survivor Advocates have applauded the Commission for its emphasis on survivor autonomy and prioritization of program utilization through reducing anticipated barriers.[3] Multiple commenters agree that the Commission should permit self-

[1] See list on cover page and in Summary.
[2] Supporting Survivors of Domestic and Sexual Violence, WC Docket No. 22-238, Notice of Proposed Rulemaking, FCC 23-9, available at https://www.fcc.gov/document/fcc-looks-help-domestic-violence-survivors-access-connectivity-0 [hereinafter "NPRM"].
[3] See, e.g., *In re* Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program, Comments of Electronic Privacy Information Center (EPIC) et al., WC Docket Nos. 22-238, 11-42, 21-450 (Aug. 18, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/1081899226693 [hereinafter "EPIC et al. NOI Comments"]; 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"].

certification of survivor status,[4] as well as a presumption of financial hardship.[5] To the extent that fraud, waste, and abuse concerns were raised by commenters,[6] these were addressed by our observation that the fraud was committed by service provider staff incentivized to commit fraud and not by subscribers themselves.[7] Commenters also observed that the Commission need not limit eligibility to one program or the other.[8] Additionally, we agree with the Asian Pacific Institute on Gender-Based Violence (API-GBV) that immigration status-related questions could have a chilling effect on applications, even if used solely for identity verification purposes.[9]

[4] Comments of CTIA, WC Docket Nos. 22-238, 11-42, 21-450 at 2, 12 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412163376283 (e.g. "Adopt survivor advocacy and direct service organizations' proposals to ensure that service providers and their front-line customer service representatives are not placed in the position of questioning the veracity of abuse survivors or mediating domestic or other abusive situations") [hereinafter "CTIA Comments"]; Comments of Verizon at 9 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412120541328 ("processes that compel or incentivize wireless providers to second-guess the user's "survivor" status, not only put providers and their employees in an untenable position but risk compromising the timeliness and certainty of the process for survivors, contrary to Congress's goals") [hereinafter "Verizon Comments"].

[5] Comments of Jara Renee Traina, WC Docket Nos. 22-238, 11-42, 21-450 at 5 (Apr. 11, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1041117409578 ("Given that 99% of survivors experience financial abuse, we believe that there should be a presumption of eligibility for survivors rather than placing additional documentation requirements to access emergency communications support.") [hereinafter "NYS OPDV Comments"]; Comments of National Lifeline Association at 5-6 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/104122601604545 ("It would be reasonable for the Commission to conclude that, based on circumstances commonly encountered by survivors of domestic and sexual violence, such survivors may have difficulty affording or acquiring access to essential communications or otherwise proving their eligibility for Lifeline.") [hereinafter "NaLA Comments"].

[6] NaLA Comments at 23-24.

[7] EPIC NNEDV et al. NPRM Comments at 15.

[8] Id. at 2; Comments of New York State Public Service Commission at 3 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/104120782330510 ("to the extent the FCC is able to choose to designate more than just one program for survivors to utilize, the NYPSC recommends the FCC expand on the directive in the Safe Connections Act and designate both Lifeline and the ACP as eligible programs"); NaLA Comments at 2 ("Given that Lifeline subscribers are also automatically eligible for ACP, expanding Lifeline eligibility will ensure that survivors gain access to both Lifeline and ACP benefits").

[9] Comments of Asian Pacific Institute on Gender-Based Violence, WC Docket Nos. 22-238, 11-42, 21-450 at 10 (Apr. 11, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412428909550 [hereinafter "API-GBV Comments"].

III. The Commission Should Consider a Discounted Device Program, No Inactivity-Triggered De-activation of Benefits, and Certain Logistical Challenges of Line Separation.

Several commenters made important points regarding the benefits survivors should be able to make use of as a result of the Safe Connections Act which may require additional attention from the Commission, namely: access to discounted devices, exemption from the standard 30-day non-usage termination of Lifeline benefits, and anticipated challenges with the logistics of line separation.

Survivor Advocates support National Lifeline Association's (NaLA's) proposal to pilot a discounted device program for survivors through the Lifeline program.[10] Carriers used to facilitate phone donations for survivors of domestic violence;[11] the Commission should explore ways it can facilitate getting survivors access to safe, functional phones if the survivor does not feel safe using their pre-existing device.

We also support NaLA's proposal to prevent survivors from having their access de-activated after 30 days of non-usage.[12] De-activating Lifeline benefits due to non-usage was appropriate when that policy was initially enacted, however in the context of survivors of domestic violence, that survivors should not be required to use their phone once per month or risk losing access. As NaLA aptly noted:

> It is clear that the value of a Lifeline service and phone for survivors could be as an emergency phone that is ready for use if and when a survivor decides to leave an abusive household or an abuser. The phone should not be turned off because the survivor failed to use it in the previous month.[13]

---

[10] NaLA Comments at 17 ("Qualifying survivors experiencing financial hardship and receiving voice and broadband service from Lifeline ETCs will need access to affordable devices, which generally means deeply discounted or free devices").
[11] See, e.g., Verizon's HopeLine Phone Program Update, ICADV (Feb. 20, 2018), https://icadvinc.org/verizons-hopeline-phone-program-update/.
[12] NaLA Comments at 20-21.
[13] NaLA Comments at 21.

Commenters also made a number of important points about the logistics of line separation. We encourage the Commission to consider NCTA's observation that: if a provider cannot create a new account for an abuser without contacting them, they should be permitted to instead create a new account for the survivor requesting the line separation.[14] Regarding CTIA's comments about incorporating standards of "commercial availability" and "technical feasibility" which might exempt providers from line separation obligations,[15] we would emphasize the Commission's proposed notice requirements for 64.6402(b).[16] However, the Commission should not permit any exemptions from the call log obligations of the Safe Connections Act; it would be too confusing and create unnecessary risk to survivors for some providers to fulfill these obligations but other providers to be exempt from them, as the Commission already explained.[17] Regarding Mobile Virtual Network Operators ("MVNO"), we urge the Commission to ensure that the obligations of each party are clear so that the MVNO and the underlying provider are not repeatedly assigning responsibility to the other. The Commission should articulate responsibilities for each party upfront, for example: the underlying carrier responsible for removing covered hotlines from call detail records,[18] the MVNO responsible for employee

[14] Comments of NCTA – The Internet & Television Association, WC Docket Nos. 22-238, 11-42, 21-450 at 4 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412457218921 [hereinafter "NCTA Comments"].
[15] CTIA Comments at 2.
[16] "(b) If a covered provider cannot operationally or technically effectuate a line separation request, the covered provider shall: (1) notify the survivor who submitted the request of that infeasibility at the time of the request or, in the case of a survivor who has submitted the request using remote means, not later than 2 business days after receiving the request; and (2) provide the survivor with information about other alternatives to submitting a line separation request, including starting a new line of service."
[17] NPRM at ¶ 115.
[18] NaLA Comments at 24-26.

training,[19] one or the other ultimately responsible for authenticating the survivor's identity,[20] and so on.

IV. The Commission Should Address Additional Privacy Concerns.

Survivor Advocates urge the Commission to address additional threats to survivor privacy and autonomy, such as "dual-use" apps (including carrier-branded family tracker apps), products and services that are strictly stalkerware fueled by CPNI from a survivor's device, employee and law enforcement misuse of access to databases containing survivor data, and Public Safety Answering Points (PSAP) access to survivor status information.

a. The Commission Should Investigate Family Tracker Apps and Similar Apps[21]

In addition to stalkerware designed expressly for that purpose (discussed further below), we urge the Commission to investigate "dual-use" apps (e.g. apps that are designed to be used as a family tracker but which abusers could leverage as functional equivalents to stalkerware), especially carrier-branded apps. Each of the three largest carriers offer this functionality, with varying degrees of notice and control to the phone subscriber who is being tracked by the "parental" account.[22] Survivor advocates have observed that these carrier-branded apps can be even harder to remove or disable than third-party stalkerware apps.[23]

---

[19] Verizon Comments at 7.
[20] Comments of Competitive Carriers Association, WC Docket Nos. 22-238, 11-42, 21-450 at 6 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412581900283; CTIA Comments at 7.
[21] Many of the citations in this section were drawn from Dr. Thomas Ristenpart's presentation "Mitigating Technology Abuse in Intimate Partner Violence and Encrypted Messaging", CITP Distinguished Lecture Series (Feb. 22, 2023), https://citp.princeton.edu/event/citp-distinguished-lecture-ristenpart/.
[22] See, e.g., "ATT Secure Family – is child texted when located?" (Nov. 21, 2018), https://forums.att.com/conversations/plans-features/att-secure-family-is-child-texted-when-located/5df00960bad5f2f606c2c58a; "T-Mobile Family Mode", https://www.t-mobile.com/offers/t-mobile-family-mode (last visited May 9, 2023); Sarah Kimmel Werle, Expert tips for using the Verizon Smart Family app (Apr. 13, 2023), https://www.verizon.com/about/parenting/expert-tips-using-verizon-smart-family-app.
[23] See, e.g., Kaofeng Lee and Erica Olsen, *Cell Phone Location, Privacy and Intimate Partner Violence*, 18 Domestic Violence Report No. 6 at 3 (Aug./Sept. 2013), https://www.acesdv.org/ wp-content/uploads/2014/06/NNEDV_CellPhoneLocationPrivacy_DVRarticle_2013.pdf ("If it is a family

The Commission's authority here is clear. These apps advertise that they track location (which is CPNI), and at a minimum carriers promote these apps if they don't outright own them (the apps often include the name of the carrier's brand). While we are optimistic that carriers are interested in developing solutions that effectively protect survivors, we note that the Commission's CarrierIQ Ruling may serve as helpful precedent for the Commission to compel the protection of survivor CPNI.[24] We would be happy to work with the Commission and with carriers to draft investigatory questions and suggest best practices to better protect survivors.[25]

For example, apps that only allow one admin account (may also be called an "owner" or "parent" account) which can turn on and off family tracking are more prone to misuse by abusers than apps that give other users autonomy. Additionally, a persistent notification[26] would better

---

locator plan that is provided through the wireless carrier, the survivor can contact the wireless carrier and ask for it to be removed. Note that only the primary account holder may be able to make these changes. …In some cases, if the abuser is alerted that the survivor knows the phone is being tracked, this may escalate the danger. If this is a concern for the survivor, then an option may be to figure out how to continue using the phone but in a way that minimizes the information that is being shared to the abuser."); Android Safety Guide, Clinic to End Tech Abuse 3 (last updated Dec. 9, 2022), https://www.ceta.tech.cornell.edu/_files/ugd/9e6719_4db0b8e8154844bf84665ad3f04ec6c6.pdf (noting that account holders may have access to what a survivor's phone is doing if the survivor is on a shared plan).

[24] *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, FCC 13-89, Declaratory Ruling at ¶ 18 (June 27, 2013), https://www.fcc.gov/document/mobile-device-cpni-declaratory-ruling ("We take this action not because the practice of collecting CPNI from customers' mobile devices is inherently improper or to prevent providers from doing so, but because these actions create risks and thus impose reasonable responsibilities on the carriers that engage in such practice"). In the context of stalkerware installed on a survivor's device by their abuser, perhaps under the guise of a family location plan, the survivor cannot be said to have assumed the risk. See id. at ¶ 32 ("While [the benefits to the consumer of being able to install apps] also come with risks to the privacy and security of consumers' information, those are risks that other parties may have a responsibility to address or that consumers might assume by their use of such applications."). We address third party apps below.

[25] At a minimum, Verizon seems receptive to this kind of discussion in the context of line separation. Verizon Comments at 17 ("Verizon welcomes guidance and input from stakeholder organizations to draw the right balance that provides survivors with critical information [regarding offerings/options] while not overwhelming them with minutiae during what is already a stressful and traumatic experience.").

[26] This is consistent with CTIA's best practices. CTIA, Best Practices and Guidelines for Location Based Services at 04(A), https://www.ctia.org/the-wireless-industry/industry-commitments/best-practices-and-guidelines-for-location-based-services (last visited May 9, 2023) ("In addition to providing notice to the account holder, LBS Providers still must ensure that notice is provided to each user or device that location

help survivors identify that they are being surveilled as opposed to a monthly text message, which can easily be intercepted and hidden, especially if it sent on a routine schedule.[27] Importantly, if a survivor knows they are being surveilled, they can take steps to protect themselves, such as leaving their phone elsewhere when visiting a family justice center, shelter, or other sensitive location.

It is also worth noting that carriers may be supporting tracking functionality through devices or apps that rely on shared location data.[28] These products or services may not advertise that they can be put towards abusive ends or caution against such risks,[29] but in other cases customer service representatives will confirm that their company's products or services can be used for these purposes.[30] Research suggests that "dual-use" apps are more prolific as tools of abusers than tools that are strictly spyware applications, and sometimes purveyors of dual-use

---

information is being used by or disclosed to the account holder or others."). See also James Gelinas, Is someone listening to everything you say? Look for this clue, Komando (Nov. 28, 2020), https://www.komando.com/privacy/is-someone-listening-to-everything-you-say-look-for-this-clue/755540/; Kishalaya Kundu, Green Dot On Android Phone: What It Means & Why It's Important, ScreenRant (updated Mar. 24, 2023), https://screenrant.com/green-dot-on-android-phone-meaning-importance/.

[27] It is important to recognize however that an abuser may have periodic access to a survivor's device and as such may be able to disable persistent notification. See, e.g., Liu, et. al., *No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps*, 2023 Proceedings on Privacy Enhancing Technologies Symposium 1, at 13 https://doi.org/10.56553/popets-2023-0013 ("The one-time 'consent' provided by the spyware installer provides largely unfettered capabilities that the true user may never be aware of."). As such, it may be advisable to require that these apps do not provide the option to disable persistent notification.

[28] See, e.g., SyncUP TRACKER, T-Mobile, https://www.t-mobile.com/support/devices/syncup-tracker-s (last visited May 9, 2023).

[29] Nicki Dell, et al, How domestic abusers use smartphones to spy on their partners, Vox (May 21, 2018), https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google ("These ['find my friends', anti-theft, and child safety apps] are 'dual use' apps. In some cases, they can be installed with the permission of the device owner and used for socially acceptable purposes. In other cases, an abuser can install them covertly on an intimate partner's device for stalking.").

[30] See, e.g., Chatterjee, et al, *The Spyware Used in Intimate Partner Violence* at 11 (May 2018), available at http://nixdell.com/papers/spyware.pdf ("Of the 9 [companies] that responded, one, TeenSafe, which is an off-store app, delivered a strong admonishment and legal warning about [Intimate Partner Surveillance (IPS)]. The other 8 responded with some version of "No, [your partner] shouldn't be able to tell [that you are tracking them via the company's app]", making them complicit in potential abuse").

apps promote their use for intimate partner surveillance (IPS) purposes.[31] While Google Play's app store seems to have taken some steps to prevent discovery of intimate partner surveillance apps through search queries in English, no such protections existed for searches in Bengali, Chinese, Hindi, Malay, Thai, and Vietnamese.[32]

Survivor Advocates urge the Commission to investigate these practices, to articulate its authority to prevent this misuse before it occurs, and to incentivize[33] meaningful notifications to users that a device or app is using the location services of the carrier's network for tracking purposes.[34]

b. The Commission Should Articulate a Preliminary List of Its Legal Authorities to Protect Survivor CPNI from Products and Services That Are Strictly Stalkerware

Regarding products or services that are strictly stalkerware, fueled by CPNI from a survivor's device—not dual-use apps that may have more than a pretextual alternative use that is not stalking, as described above—we encourage the Commission to explore and articulate its authorities. For example, the Commission could use its authority under Title III and under 47 U.S.C. 605 to declare stalkerware a *per se* unauthorized transmission by which abusers and/or app developers and sellers cause the tower ping or satellite communication to be published

[31] See, e.g., id.; Roundy, et al, *The Many Kinds of Creepware Used for Interpersonal Attacks*, 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 626-643, doi: 10.1109/SP40000.2020.00069, at 10, nixdell.com/papers/Creepware_IEEE_SandP_ camera.pdf ("correlation data shows that many apps that purport to be intended for child online safety have highest PMI with apps that are unambiguously intended for intimate partner surveillance. It is unsurprising that the 'Family Locator for Android' app appears alongside abuse apps, as its previous title was 'GirlFriend Cell Tracker.' ").

[32] Almansoori, et al, A Global Survey of Android Dual-Use Applications Used in Intimate Partner Surveillance, 2022 Proceedings on Privacy Enhancing Technologies Symposium 4, at 1, https://pages.cs.wisc.edu/~chatterjee/papers/pets22-global-dual-use-apps.pdf.

[33] It is worth noting that mobile phone OS companies are already moving in this direction. See, e.g., Kif Leswing, Apple and Google team up to stop unwanted AirTag tracking, CNBC (May 2, 2023), https://www.cnbc.com/2023/05/02/apple-and-google-team-up-to-stop-unwanted-airtag-tracking.html.

[34] In the case of apps that are strictly stalkerware, which we discuss further in Section IV(b) below, 13/14 apps studied hid the app icon from the app launcher. See Liu, et al. note 27 *supra* at 4, 7.

without the express permission of the party transmitting, thereby hijacking a phone's communications in a manner not authorized by the carrier.[35] The Commission might also consider invoking its ancillary jurisdiction to implement protections for survivors from stalkerware, arguing that it would frustrate Congress' purposes in passing the Safe Connections Act if the Commission did not take action against the transmission of survivor location data, for example. Just as the Commission has issued orders preventing carriers from perpetuating illegal robocall traffic from bad actor upstream providers,[36] the Commission could issue orders to carriers preventing the transmission of location data through applications that have been identified as strictly bad actor stalkerware apps.[37] Similarly, the Commission could require carriers to comply with survivor requests to disable any location data collection that is not strictly necessary to provide cellular voice and messaging service, including requests initiated by a survivor but made through a law enforcement organization.

c. The Commission Should Require Carriers to Protect Survivor Data from Unauthorized Access by Law Enforcement or Their Own Employees

Survivor Advocates agree with commenters who call for no disclosure of survivor data without a judicial or grand jury order (i.e. an administrative subpoena should not be sufficient).[38] Indeed, just in the 30 days since we filed our initial comment, another story broke regarding

[35] The Commission exercised this authority in the context of Google WiFi packet sniffing, see, e.g., *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. Although the Commission found an insufficient factual basis to enforce Section 705 of the Communications Act (47 USC 605) against Google, stalkerware presents a different, but related, fact pattern. The facts from the Commission's investigation suggested that Google never made use of the information that it collected. Indeed, Google alleged that it had not been aware that it was collecting the data and that it took actions to prevent the data collection once it learned the collection was occurring. Conversely, purveyors of stalkerware profit from building tools designed specifically to collect and disclose data to third parties without the user's knowledge.
[36] See, e.g., *In re* One Eye LLC, EB-TCD-20-00031678, DA 23-389, Final Determination Order (May 11, 2023), https://www.fcc.gov/document/fcc-issues-first-ever-roboblocking-order-against-one-eye.
[37] We do not think it would be appropriate for carriers to have total authority to determine what apps a user can have on their phone.
[38] API-GBV Comments at 5.

widespread law enforcement misuse of access to confidential data, including spying on exes, giving family members access to their accounts, and selling data to criminals.[39] While these kinds of privacy harms should be avoided generally, in particular the Commission cannot allow these breaches to happen with survivor data.

We also agree with commenters who call for restricting employee access to information about line separation requests, and for providing extensive training to employees who need access.[40] There is also a long history of carrier employees misusing their ability to access subscriber data.[41]

While procedural and technical safeguards can help, the most effective method is data minimization: never collecting more data than is strictly necessary, and deleting data immediately once it is no longer necessary for its original purpose. The Hotline embodies this approach, which it articulates in its comments: the cost of anonymous caller ID, texts, and web interactions is secondary to the gains for survivor safety.[42]

d. It Is Inappropriate to Flag 911 Calls as Coming from a Separated Line

One commenter urged that any calls to PSAPs from separated lines should be flagged as such, arguing that first responders should know that they're responding to a domestic relations

[39] Dhruv Mehrotra, ICE Records Reveal How Agents Abuse Access to Secret Data, WIRED (Apr. 17, 2023), https://www.wired.com/story/ice-agent-database-abuse-records/ ("According to an agency disciplinary database that WIRED obtained through a public records request, ICE investigators found that the organization's agents likely queried sensitive databases on behalf of their friends and neighbors. They have been investigated for looking up information about ex-lovers and coworkers and have shared their login credentials with family members. In some cases, ICE found its agents leveraging confidential information to commit fraud or pass privileged information to criminals for money."); EPIC NNEDV et al. NPRM Comments at App'x 2.

[40] NYS OPDV Comments at 4; NCTA Comments at 2, 8.

[41] See, e.g., *In re* Data Breach Reporting Requirements, Reply Comments of Electronic Privacy Information Center (EPIC) et al., WC Docket No. 22-21 at 3-5 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814.

[42] Comments of The National Domestic Violence Hotline, WC Docket Nos. 22-238, 11-42, 21-450 at 3 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10412702200472.

911 call.[43] This is inappropriate for at least two reasons. First, law enforcement biases about survivor claims of abuse are well-documented,[44] and this kind of notification could inappropriately color the treatment of emergency calls made by survivors, especially survivors who self-certify their status. Second, if the caller is contacting the PSAP for an emergency unrelated to their abuser (e.g. they were in a car accident with another driver, or they are calling on behalf of someone else who is injured), there is no need for their status as a survivor to be disclosed to the first responders. This is an issue of not only data minimization, but also of survivor autonomy: survivors should be in control of who knows what and when.

V. Conclusion

Survivor Advocates appreciate the opportunity to file reply comments to the Commission's NPRM on supporting survivors of domestic violence.

Respectfully submitted, this the 12th day of May 2023, by:

Chris Frascella
Law Fellow
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036
frascella@epic.org

Erica Olsen
Safety Net Senior Director
National Network to End Domestic Violence
1325 Massachusetts Ave NW, 7th Floor
Washington, DC 20005-4188
eo@nnedv.org

Lana Ramjit
Dir. Operations
Clinic to End Tech Abuse
2 West Loop Rd
New York, NY 10044
lana.ramjit@cornell.edu

Nick Garcia
Policy Counsel
Public Knowledge
1818 N St, Suite 410
Washington, DC 20036
nick@publicknowledge.org

[43] Comments of Boulder Regional Emergency Telephone Service Authority, WC Docket Nos. 22-238, 11-42, 21-450 at 3-4 (Apr. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10413004724587.
[44] EPIC et al. NOI Comments at 3-4.