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
	)	

COMMENTS ON NOTICE OF PROPOSED RULEMAKING

by

Electronic Privacy Information Center (EPIC),
National Network to End Domestic Violence (NNEDV), and
Cyber Civil Rights Initiative (CCRI),
Clinic to End Tech Abuse (CETA),
Electronic Frontier Foundation (EFF),
Iowa Coalition Against Domestic Violence (ICADV),
National Coalition Against Domestic Violence (NCADV),
National Consumer Law Center (NCLC), on behalf of its low-income clients,
The National Domestic Violence Hotline,
National Resource Center on Domestic Violence (NRCDV),
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 April 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

Jessie, Safety Net Technology Safety Specialist
NNEDV

Summary

The Commission's Notice of Proposed Rulemaking (NPRM) implementing the requirements of the Safe Connections Act is an encouraging step forward. Through the NPRM, the Commission addresses an issue that demands attention with an awareness of the unique needs and challenges faced by survivors.

We offer the following three principles to assist the Commission in staying true to this approach: maximize survivor self-determination and agency; maximize program utilization and access by minimizing burdens and barriers for survivors; and protect survivors by prioritizing data minimization. Self-attestation of survivor status and financial hardship is essential to all three of these principles. Self-attestation does not require survivors to engage third-party services in order to benefit from the Commission's programs (which can implicate equity issues); to rely on others to vouch that the trauma they experienced is real; or to submit personal information that survivors might not have the ability to access, and that if exposed, could put survivors' lives at risk.

We support the Commission's inquiry regarding waiting and weighing whatever evidence of fraud, waste, and misuse may or may not ultimately present itself, rather than pre-emptively introducing barriers that might inhibit survivor utilization of its programs. We also support the Commission's proposal to create a registry of hotlines, shelters, and other organizations—interpreting "hotline" broadly—that would be automatically omitted from customer-facing records (such as call logs).

We further urge the Commission to prioritize data minimization and to require carriers to implement data security best practices for the entire duration that any data retention is necessary, better protecting the safety and privacy of survivors by safeguarding their data. For similar reasons, we reiterate the concerns initially voiced in our NOI comments regarding misuse of law

enforcement access to survivor data. Appendix 2 documents a non-exhaustive list of instances of this misuse; this problem is not clearly limited to a small percentage of law enforcement staff nor to a specific geography. We also applaud the Commission's willingness to address on-device safety issues for survivors, such as stalkerware, and offer suggestions for how the Commission might help carriers to better support phone subscribers concerned about this issue.

After a brief introduction, these comments begin with addressing survivor self-determination and agency (Section II); articulate support for the Commission's efforts to minimize burdens and barriers for survivors, identify room for improvement, and urge the Commission to prioritize accessibility and utilization over fraud prevention (Section III); support the Commission's efforts to require data minimization and adequate data security (Section IV); urge the Commission to account for misuse of law enforcement access to survivor data (Section V); recommend the Commission offer guidance to carriers regarding stalkerware (Section VI); and support the Commission's broad interpretation of "hotline" (Section VII).

Table of Contents

Comments

I. Introduction

The Federal Communications Commission (FCC, or "Commission") seeks comment on its Notice of Proposed Rulemaking (NPRM) regarding how it might better support survivors of domestic and sexual violence (hereinafter "domestic violence") through its implementation of the Safe Connections Act.[1] The **Electronic Privacy Information Center (EPIC)**, **the National Network to End Domestic Violence (NNEDV)**, and the undersigned survivor advocacy and direct service organizations[2] submit these comments to emphasize the importance of the Commission's proposals and to suggest further improvements, including self-attestation from survivors, data minimization best practices, protecting survivor data from misuse via law enforcement access, assisting carriers in protecting survivors from stalkerware, and creating a registry of hotlines (broadly understood) to be omitted from customer-facing records.

As in EPIC et al.'s comments to the Commission's related Notice of Inquiry (NOI),[3] here we applaud the Commission not only for its attention to this issue but also for its clearly well-considered, open-minded, and empathetic approach. We urge the Commission to keep at the forefront of its mind: maximizing self-determination and agency of survivors; minimizing burdens and barriers that may limit survivors' use of the benefits of the Commission's proposed programs; and minimizing the amount of information collected, retained, and disclosed about

---

[1] 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"].
[2] See Appendix 1 for descriptions of the organizations joining in these comments.
[3] *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"].

survivors by all entities concerned (including local shelters, telecom providers, and law enforcement).

II. The Commission's Proposals Rightly Emphasize Survivor Self-Determination and Agency.

We support the Commission's proposals that maximize survivor self-determination and agency. Such proposals include assistance with line separation requests from supportive services providers,[4] survivors designating their preferred means of communication,[5] ensuring that survivors who reach out for assistance with line separation aren't subject to marketing efforts,[6] allowing survivors to select which program (Lifeline or the Affordable Connectivity Program (ACP)) would best support them,[7] and providing flexibility in terms of service plans, number portability, devices, and means of submitting line separation requests.[8] These measures give survivors the ability to take what assistance they need, in the manner they need it, when they need it; as Commissioner Starks noted: "[o]ne 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."[9]

We encourage the Commission to continue to identify ways to support survivors' self-determination and agency, such as allowing for self-attestation.[10] Requiring that survivor status

---

[4] NPRM at ¶ 64.
[5] Id. at ¶ 52.
[6] Id. at ¶¶ 55, 76.
[7] Id. at ¶ 154.
[8] Id. at ¶¶ 62, 76, 79-85, 174.
[9] 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.
[10] NPRM at ¶ 158.

be verified by a third-party creates a chilling effect and places a significant burden on survivors who need this critical assistance but who may not be currently receiving services nor be in a position to request documentation of their experience from particular, specialized third parties (like law enforcement, a court, or a licensed medical provider).[11] It may also be unsafe for a survivor to access services offered by a third party without first having an independent means of communication they would not be able to obtain but for a line separation. Consistent with our NOI comments, here again we urge the Commission to let each individual survivor decide when and to what extent they take advantage of the resources available to them.[12]

III. The Commission Should Continue to Minimize Burdens and Barriers for Survivors, to Maximize Program Utilization.

We again acknowledge and applaud the Commission's thoughtfulness and thoroughness in its rulemaking. An abusive partner can attempt to exert control over a survivor in various ways, and the Commission's questions and proposals reflect an understanding of this dynamic. We urge the Commission to make it as easy as possible for survivors to take advantage of its programs by prioritizing access and utilization first and foremost; also ensuring survivors are prepared for and supported during transition periods; and addressing issues of fraud, waste, and misuse only to the extent that they become apparent to the Commission as outweighing the gains achieved for legitimate beneficiaries.

---

[11] Requiring third-party certification would be tantamount to requiring the survivor to engage other supportive services, thereby undermining survivor agency. Section III(b) below also addresses the equity issues with this proposal for survivors who may not have the ability to readily engage supportive services even if they would like to. We further note that in some instances it is precisely because a survivor has had a negative interaction with these third-parties in the past that they might feel uncomfortable seeking documentation from them.

[12] EPIC et al. NOI Comments at 2-5.

We support the Commission's proposals that prioritize program accessibility and utilization by minimizing the burdens and barriers that might prevent or discourage survivors from engaging in programs authorized by the Safe Connections Act. These proposals include accommodating the unique challenges and vulnerabilities often faced by survivors—for example an impeded ability to obtain documents[13] and an elevated need to keep their location private—by accepting alternative forms of verification of identity,[14] survivor status,[15] income documentation,[16] and address information.[17] Such proposals also include definitions broad enough to avoid excluding eligible survivors from program participation by, for example:

- including caretakers of survivors among those who can initiate line separation,[18]
- not limiting line separation to group plans in which the abuser is the primary account holder,[19]
- recognizing that permitting survivors to only ever rely on programs once and for up to a six-month maximum period during their entire lifetime is unrealistic,[20] and

[13] Anecdotally, Iowa supportive services providers have estimated to their state coalition that approximately 90% of survivors who come to them seeking services need help replacing documents and applying for SNAP benefits. These providers further emphasize that making eligibility for the Commission's programs contingent upon SNAP eligibility would not improve accessibility because survivors need help from supportive services providers replacing eligibility documents just to apply for SNAP.
[14] NPRM at ¶¶ 44, 45.
[15] Id. at ¶ 48, 49.
[16] Id. at ¶¶ 157-61.
[17] Id. at ¶¶ 46, 165-66, 178.
[18] Id. at ¶¶ 23, 24, 36.
[19] Id. at ¶ 35.
[20] Id. at ¶ 173.

- treating the temporary emergency communications support as low risk for fraud, waste, or misuse.[21]

To further address unique challenges faced by survivors, we also encourage the Commission to incentivize communications service providers to train their employees to assist survivors in detecting and removing stalkerware.[22] We disagree with the Commission's proposals and inquiries that would allow telecom service providers discretion on implementation of programs, which could result in further limitations to survivor access to programs,[23] and urge the Commission to consider offering guidance to carriers in supporting survivors in transitioning out of benefits scheduled to imminently terminate.[24]

a. The Commission Has Made Some Great Strides in Minimizing Burdens and Barriers for Survivors

Many of the Commission's proposals reflect an understanding of the challenges faced by survivors. Some of these challenges include limited access to documents and finances, sensitivity of location information, non-uniformity in terms of their support systems,[25] and limited information about how phone group plans may be structured. The Commission's proposals seem to reflect a genuine, thoughtful effort to ensure that survivors receive the support they need despite these challenges.

---

[21] Id. at ¶ 158.
[22] See Section VI below.
[23] *See, e.g.*, NPRM at ¶¶ 43, 45, 50.
[24] *See* EPIC et al. NOI Comments at 12-14. *See also* Chris Frascella and Erica Olsen, What the FCC's Safe Connections Rule Must Get Right to Support Survivors of Domestic Violence, epic.org (Mar. 16, 2023), https://epic.org/what-the-fccs-safe-connections-rule-must-get-right-to-support-survivors-of-domestic-violence/.
[25] *See, e.g.*, NPRM at ¶ 64.

We support the Commission's proposals to adopt expansive definitions of "covered act",[26] "survivor",[27] "covered provider",[28] and "covered hotline."[29] We also support the Commission's proposed interpretation that neither the abuser nor the survivor must be the primary account holder on a group plan for the survivor to be eligible to request a line separation under the Safe Connections Act.[30] An alternative interpretation might exclude survivors whom Congress intended to protect through these programs.

We support the Commission's proposal to permit alternative forms of verification in light of the fact that survivors may not be able to obtain documents required under the Safe Connections Act.[31] Similarly, we support the Commission's prohibition of making line separation contingent upon a survivor credit check or other estimation of survivor's ability to pay,[32] and the Commission's presuming financial hardship.[33] We also support the Commission's proposals for survivors to provide alternative information in their Lifeline or Affordable Connectivity Program (ACP) applications due to the increased risks they face if their personal data, such as location data, is exposed.[34]

---

[26] Id. at ¶ 20.
[27] Id. at ¶¶ 24-25.
[28] Id. at ¶ 28.
[29] Id. at ¶¶ 126-128.
[30] Id. at ¶ 35.
[31] Id. at ¶ 49.
[32] Id. at ¶ 88.
[33] Id. at ¶¶ 157-58.
[34] Id. at ¶¶ 165-66.

b. Additional Practices the Commission Should Adopt to Prioritize Accessibility and Utilization

We support the Commission's efforts to ensure all survivors can access and utilize the programs under the proposed rule and urge the Commission to remove additional barriers.

1. Presumption of financial hardship or self-certification

The Safe Connections Act does not impose requirements based on financial hardship nor does it define financial hardship.[35] As a result, the Commission should presume financial hardship where survivor status has been attested to.[36] A presumption of financial hardship would enable programs to reach more survivors by removing the obstacles associated with demonstrating financial instability.[37]

If the Commission is going to routinize the application process for programs and decline to presume financial hardship, we encourage the Commission to permit survivors to self-certify that they need access to its temporary assistance programs because they are either under a certain income level or have lost access to funds such that they require temporary assistance. As the Commission notes, the fact that the assistance is temporary reduces the risk of waste, fraud, or misuse connected with survivor self-certification.[38] The Commission should model its policies after the Department of Housing and Urban Development's self-certification policies, which help survivors maintain housing subsidy and occupancy.[39]

---

[35] Congress did indicate in its findings that survivors face barriers such as financial insecurity. *See* Safe Connections Act Section 3(2), available at https://www.congress.gov/bill/117th-congress/house-bill/7132/text.
[36] NPRM at ¶ 157.
[37] Id. at ¶ 159.
[38] Id. at ¶ 158.
[39] *See, e.g.*, HUD Expands Housing Protections for Survivors of Violence, HUD Archives: News Releases (Oct. 24, 2016), available at https://archives.hud.gov/news/2016/pr16-159.cfm.

Self-certification is preferable to third-party certification, which imposes barriers for survivors.[40] Many survivors never actually seek services.[41] This includes but is not limited to LGBTQ+,[42] indigenous,[43] immigrant,[44] Asian-American,[45] Jewish,[46] and male survivors,[47] as

---

[40] *See* EPIC et al. NOI Comments at 7-9.
[41] Reagan Greenberg, *The "Particular Social Group" Requirement: How the Asylum Process is Consistently Failing LGB Applicants and How an Evidentiary Standard of "Self-Attestation" Can Remedy These Failures*, 17 U. Md. L. J. of Race, Relig., Gender, and Class 147 (2017), available at: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1283&context=rrgc (noting importance of self-attestation for equity in the asylum process for marginalized groups, especially for queer people). Greenberg's work is in the asylum-seeking context, but the same rationale applies here. *See, e.g.*, EPIC et al. NOI Comments at 4, 6-7, 13.
[42] Jenna M. Calton, Lauren Bennett Cattaneo and Kris T. Gebhard, Barriers to Help Seeking for Lesbian, Gay, Bisexual, Transgender, and Queer Survivors of Intimate Partner Violence, 17 Trauma, Violence & Abuse 585 (Dec. 2016), available at: https://www.jstor.org/stable/26638153.
[43] Renee Fiolet, Laura Tarzia, Mohajer Hameed, and Kelsey Hegarty, *Indigenous Peoples' Help-Seeking Behaviors for Family Violence: A Scoping Review*, 22 Trauma, Violence & Abuse 370 (May 30, 2019), available at: https://journals.sagepub.com/doi/abs/10.1177/1524838019852638.
[44] Eben M. Ingram, *A Comparison of Help Seeking Between Latino and Non-Latino Victims of Intimate Partner Violence*, 13 Violence Against Women 159 (Feb. 1, 2007), available at: https://journals.sagepub.com/doi/abs/10.1177/1077801206296981.
[45] Hyunkag Cho, Use of Mental Health Services Among Asian and Latino Victims of Intimate Partner Violence, 18 Violence Against Women 404 (June 13, 2012), available at: http://news.msu.edu/media/documents/2012/07/348be18c-e909-4e99-a951-8cc5c4a57476.pdf ; Hyunkag Cho, Woo Jong Kim, *Intimate Partner Violence Among Asian Americans and Their Use of Mental Health Services: Comparisons with White, Black, and Latino Victims*, 14 Journal of Immigrant and Minority Health 809 (Apr. 22, 2012), available at: http://news.msu.edu/media/documents/2012/07/b4652c5c-5d22-4283-88b8-c72528c87b17.pdf.
[46] Shalom Bayit, Jewish Family Service Calgary (JFSC), https://www.jfsc.org/programs--services/domestic-violence---shalom-bayit.html (last visited Apr. 10, 2023) (summarizing Letourneau, et al., Domestic Abuse in the Jewish Communities of the Canadian Prairie Province of Calgary (Feb. 19, 2019), available at: https://www.boffinaccess.com/nursing-practice-and-healthcare/domestic-abuse-in-1-102); Jewish Women International, *A Portrait of Domestic Abuse in the Jewish Community: Key Findings from the National and Chicagoland Needs Assessments* (May 2004), available at: https://issuu.com/jewishwomeninternational/docs/nna_summary_report_pdf.
[47] Cho and Kim, *supra* note 45.

well as survivors experiencing financial insecurity.[48] Survivors in rural areas may need to traverse three times the distance to reach the nearest supportive services program.[49] Requiring third-party certification would predictably result in inequitable access to the Commission's programs.

Third-party certification also forces staff at survivor support organizations to become responsible for investigating the survivor's finances. Not only is this a burden on top of their many pre-existing responsibilities as a direct services provider,[50] but it is also an inappropriate role that raises a host of other issues including potential liability if they get it wrong; collecting more financial data than is necessary in order to avoid liability for getting it wrong; and navigating confidentiality obligations from federal funding programs which would likely require a written, time-limited, and informed release from the survivor.[51] In short: it would be both burdensome and counter-productive.

---

[48] Id.

[49] Corinne Peek-Asa, et al., *Rural Disparity in Domestic Violence Prevalence and Access to Resources*, 11 J. Womens Health (Larchmt) 1743 (Nov. 2011), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3216064/?mod=article_inline ("The mean distance to the nearest IPV resource was three times greater for rural women than for urban women, and rural IPV programs served more counties and had fewer on-site shelter services. Over 25% of women in small rural and isolated areas lived >40 miles from the closest program, compared with <1% of women living in urban areas.").

[50] Shanti Kulkarni, et al., *Exploring Individual and Organizational Factors Contributing to Compassion Satisfaction, Secondary Traumatic Stress, and Burnout in Domestic Violence Service Providers*, 4 J. of the Society for Social Work and Research 114 (June 3, 2013), https://www.journals.uchicago.edu/doi/pdf/10.5243/jsswr.2013.8 (DV advocates rated workload lowest of all metrics of work-life satisfaction surveyed by the Areas of Worklife Scale, at only 2.89 on a 1-5 scale).

[51] Lonne, Robert L., *Social workers and human service practitioners* (2003), in: Dollard, Maureen F. and Winefield, Anthony H. and Winefield, Helen R., (eds.) *Occupational Stress in the Service Professions*, Taylor & Francis, London, pp. 281-310,

If the Commission decides to require income documentation as proof of financial hardship (an outcome we discourage), we urge the Commission to give survivors 60 days from the day they begin using the service to provide the necessary documentation, with the opportunity to apply for an extension beyond the initial 60 days.[52]

2. Transitional support for survivors

We support the Commission's proposal to put a transition plan in place to assist survivors who are approaching an imminent termination of their benefits under the Safe Connections Act,[53] and to permit multiple periods of support over the lifetime of the survivor.[54] Indeed it would be contrary to the goals of the Safe Connections Act to limit survivors to only one period of support, up to six months in length, when there is clear evidence that it can take 7 attempts or more for a survivor to permanently leave an abusive partner.[55]

---

available at: https://eprints.qut.edu.au/20086/1/c20086.pdf (noting role conflict, i.e. being tasked with roles that conflict with each other, and role ambiguity as factors in burnout and work stress among human services practitioners).

[52] NPRM at ¶ 161.

[53] Id. at ¶ 175.

[54] Id. at ¶ 173.

[55] Why It's So Difficult to Leave, Women Against Abuse, https://www.womenagainstabuse.org/education-resources/learn-about-abuse/why-its-so-difficult-to-leave (last visited Apr. 10, 2023); Mindy B. Mechanic, et al., The Impact of Severe Stalking Experienced by Acutely Battered Women: An Examination of Violence, Psychological Symptoms and Strategic Responding, 15 Violence and Victims 443 (Oct. 29, 2010), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2966386/ (noting that 30% of infrequently stalked battered women and 65% of those relentlessly stalked reported 6 or more prior attempts to leave the relationship, with 24% of relentlessly stalked women reporting 16 or more prior attempts before they were able to successfully leave the relationship).

Additionally, six months is unlikely to be sufficient time for a survivor to establish financial independence and stability.[56] As Network of Victims Recovery of DC (NVRDC) noted in their comments in response to the Commission's NOI, three years would be the ideal duration to adequately support survivors.[57] If the Commission must impose a period of fewer than three years, it should scale up its eligibility requirements over time and provide transition support, rather than requiring demonstrations of eligibility survivors may not be able to satisfy initially and leaving survivors to face an "all or nothing" cliff at the end of their initial period of eligibility.

3. Prohibition of additional requirements by telecom service providers

The Commission asks whether the Safe Connections Act allows telecom providers to put their own processes in place (e.g., verification) on top of the Commission's own rules.[58] We maintain that it does not. The Safe Connection Act as enacted in 47 U.S.C. 345(b)(2) states that "a covered provider may not make separation of a line from a shared mobile service contract

---

[56] Frascella and Olsen, *supra* note 24 ("This transition time will be a critical timeframe for establishing accounts and practices with privacy and safety in mind."); EPIC et al. NOI Comments at 13-14 ("Additionally, the six-month allowance in the Safe Connections Act may not be sufficient for a survivor to establish financial independence and stability.") (citing to the successes of continuous eligibility in the Medicaid coverage context); id. at 13 n 45 ("although the average stay in an emergency homeless shelter is only 60 days, the average length of time it takes a homeless family to secure housing is closer to 6-10 months.") (citing to Domestic Violence, Housing, and Homelessness, National Network to End Domestic Violence (NNEDV) (July 2019), https://nnedv.org/wp-content/uploads/2019/07/Library_TH_2018_DV_Housing_Homelessness.pdf); *In re* Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program, Comments of Network of Victims Recovery of DC, WC Docket Nos. 22-238, 11-42, 21-450 at 8 (Aug. 18, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/10818306215260 [hereinafter "NVRDC NOI Comment"].

[57] NVRDC NOI Comment at 8.

[58] NPRM at ¶¶ 43-45, 50.

…contingent on any requirement other than the requirements [requiring a survivor to submit verification of survivor status and of the phone line to be separated].” The Commission should interpret this to mean that a covered provider may reject a line separation request that is not accompanied by any verification of survivor status or of the phone line to be separated, but not to mean that each individual provider is entitled to narrow what constitutes adequate verification (beyond their input throughout this rulemaking process).

The Commission is responsible for the determination of what minimum certifications survivors must provide, as its proposals throughout this NPRM imply.[59] Moreover, this is a particularly vulnerable population seeking critical services in a market in which competition is unlikely to motivate industry behavior; providers would likely not improve accessibility solely to attract the business of survivors. Nor would it be appropriate to place the burden on survivors to comparison shop. Accordingly, the Commission must establish parameters to ensure carriers do not frustrate program accessibility and utilization.

While providers should not be permitted to impose additional requirements, providers should be empowered to offer alternative methods of certification in the interest of promoting accessibility and utilization. If providers want to offer additional methods of verification that they believe balance survivor accessibility and consumer protections against fraud, the providers should be free to do so—so long as any one method is sufficient to fulfill a line separation request (and does not violate other principles, such as survivor confidentiality).[60]

---

[59] Id. at ¶ 85.
[60] Id. at ¶ 45.

The parameters the Commission establishes for telecommunications services providers should require providers to make accommodations for survivors who do not have access to identification documents, who do not have a permanent address apart from their abuser's, and/or who may opt not to provide such sensitive information. (This privacy concern may also extend to their Social Security Number, as the Commission notes.)[61] Because Congress explicitly preserved the rights of states to set less stringent requirements for line separation,[62] the Commission should similarly be explicit with communications services providers that the lists of affidavits and of records offered in § 345(c)(1)(A) are non-exhaustive. These lists rely on access to licensed professionals or to the decision to utilize such resources as well as to work with law enforcement (and may rely upon being believed by law enforcement).[63] The Commission should not be so prescriptive about what resources a survivor engages and when; we again emphasize the issues of self-determination and equity that should take priority in this proceeding.[64] We further note that the Safe Connections Act does not define "official record that documents the covered act [of abuse],"[65] leaving room for interpretation, and explicitly does not require the determination of a court for an act to trigger the Safe Connections Act's protections.[66]

---

[61] Id. at ¶ 46.
[62] Id. at ¶ 49.
[63] *See, e.g.*, 47 USC § 345(c)(1)(A)(ii) ("a copy of a police report, statements provided by police"); The National Domestic Violence Hotline, Who Will Help Me? Domestic Violence Survivors Speak Out About Law Enforcement Responses, at 3-5, 7-8, 10 (2015), https://www.thehotline.org/wp-content/uploads/sites/3/2015/09/NDVH-2015-Law-Enforcement-Survey-Report.pdf.
[64] See Section II, III(b) above.
[65] 47 USC 345(c)(1)(A)(ii).
[66] 47 USC 345(a)(2)(B).

Where an application is rejected, we support the Commission's proposal to impose a two-business-day timeframe on resubmissions.[67] Time may be of the essence when a survivor initiates the line separation request, and there is no reason a provider expected to respond within two days of the initial submission cannot respond within two days for subsequent submissions.

We also re-iterate the concerns voiced in API-GBV's NOI comments about language barriers—lack of meaningful language access can further isolation created by an abuser.[68] The Safe Connections Act requires that covered providers notify survivors seeking line separation that the provider may contact the survivor in "clear and accessible language."[69] We urge the Commission to extend this "clear and accessible" requirement to any communications between providers and survivors, including requiring providers to communicate in the survivor's preferred language if the provider has published marketing materials or conducting marketing outreach in that language.[70]

---

[67] NPRM at ¶ 38.

[68] *In re* Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program, Comments of Asian Pacific Institute on Gender-Based Violence, WC Docket Nos. 22-238, 11-42, 21-450 at 4-5 (Aug. 18, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/10819301721882 [hereinafter "API-GBV NOI Comment"].

[69] 47 USC 345(c)(2)(A).

[70] The requirement that the line separation mechanism be "easily navigable" and information be "readily available" may also be relevant to language access concerns here. NPRM at ¶¶ 61-62, 65-67. *See also Empowering Broadband Consumers Through Transparency*, CG Docket No. 22-2, Report and Order and Further Notice of Proposed Rulemaking, FCC 22-86, at ¶ 134, available at https://docs.fcc.gov/public/attachments/FCC-22-86A1.pdf (requiring ISPs to make broadband nutrition labels available in English and any other languages in which they market their services in the United States).

4. Prioritization of program accessibility

Survivors should not be prevented from accessing and utilizing the programs for fear of fraud.[71] We agree with API-GPV[72] that until evidence demonstrates the need for stronger fraud prevention to authenticate the identity of a survivor, the appropriate balance is to err on the side of accessibility and utilization. A 2015 GAO white paper on combatting fraud in federal programs also suggests that *impact* of fraud should be a relevant factor, not merely *likelihood* of fraud,[73] and identifies "residual risk" as part of the process of prioritizing new control activities to reduce unacceptable risks of fraud to a tolerable level.[74] This seems to counsel in favor of gathering more information about the impact of fraud before implementing measures that may discourage program participation. Regarding likelihood specifically, we note that the Commission's November 2019 Lifeline Report and Order identifies telecommunications providers' own representatives, who were incentivized to enroll ineligible users, as a source of "much of the fraud, waste, and abuse in the Lifeline program"—not subscribers themselves.[75] The Order prohibited these incentives[76] and required registration of enrollment representatives to prevent further instances of this behavior.[77]

---

[71] NPRM at ¶ 44.
[72] See API-GBV NOI Comment at 6.
[73] Government Accountability Office, A Framework for Managing Fraud Risks in Federal Programs 14 (July 2015), https://www.gao.gov/assets/gao-15-593sp.pdf.
[74] Id. at 15.
[75] Bridging the Digital Divide for Low-Income Consumers, Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, WC Docket Nos. 17-287, 11-42, 09-197, Fifth Report and Order, Memorandum Opinion and Order and Order on Reconsideration, and Further Notice of Proposed Rulemaking, at ¶ 69; id. at ¶ 72.
[76] Id. at ¶ 68.
[77] Id. at ¶¶ 79-81.

5. Removal of any added friction in the application process

The Commission should enact regulations designed to reduce friction caused by things like bothersome distractions, lengthy forms, and unnecessary data collection. Prospective program participants in any program are less likely to engage if there is friction in the process of achieving their goal. For example, website visitors are less likely to remain on a website if bombarded by pop-up ads;[78] survey-takers are less likely to complete longer questionnaires;[79] and customers are often dissuaded from cancelling or changing a service when companies use impediments in their call centers such as long wait times, Voice Recognition Units (VRUs), and customer reclamation teams.[80] Survivors face even more friction and are more likely to feel too overwhelmed to continue when these types of activities are combined with experiences of trauma, heightened stress, and heightened sensitivity to the privacy of their personal information.[81] The Commission should strive to avoid a cumbersome stressful process for applicants to its programs, and as a result, we encourage the Commission to address additional unnecessary barriers so more survivors will benefit from the Commission's programs.

---

[78] *See, e.g.*, Mimi An, Why People Block Ads (And What It Means for Marketers and Advertisers), HubSpot (July 13, 2016, updated Jan. 14, 2020), https://blog.hubspot.com/marketing/why-people-block-ads-and-what-it-means-for-marketers-and-advertisers (noting 64% of people use ads blockers because "ads disrupt what I'm doing," pop-up ads have a 73% disapproval rating).

[79] *See, e.g.*, Brent Chudoba, How much time are respondents willing to spend on your survey?, SurveyMonkey, https://www.surveymonkey.com/curiosity/survey_completion_times/ (last visited Apr. 12, 2023) (noting surveys that took more than 7-8 minutes were 5-20% less likely to be completed).

[80] *See, e.g.*, Jim Kreidler, Tried to cancel a service but couldn't? Learn steps to take, Fed. Trade Comm'n Consumer Alert (Nov. 3, 2022), https://consumer.ftc.gov/consumer-alerts/2022/11/tried-cancel-service-couldnt-learn-steps-take.

[81] EPIC et al. NOI Comments at 3-5, 7, 14.

c. The Commission Should Safeguard Against Fraud, But Not at the Expense of Survivor Accessibility

The Commission asks about fraud prevention measures to ensure its programs aren't manipulated by scammers (or abusers) for nefarious purposes. These measures include authentication and notification. We maintain that line separation on its own does not implicate the same consequences as SIM swapping or port-out fraud. We support authentication based on any phone number on a group plan rather than the primary account holder's phone or address. And we support survivor-directed notification.

We continue to agree with the Commission that greater safeguards are necessary to protect consumers from SIM swapping and port-out fraud.[82] We ask the Commission distinguish between (1) fraud which directly intercepts communications (including two-factor authentication messages, which can lead to compromise of financial accounts and other personal information) such as SIM swapping and port-out fraud,[83] and (2) transferring an account from a group plan to individual ownership. We recognize that a change in ownership can complicate undoing the harm perpetrated by a SIM- or port-out-based fraud, as that becomes a second knot for the fraud victim to untangle. However, the Commission's efforts to prevent frauds that intercept

---

[82] NPRM at ¶ 44. *See also* In re *Protecting Consumers from SIM Swapping and Port-Out Fraud*, Comments of NCLC and EPIC, WC Docket No. 21-341 (Nov. 15, 2021), https://www.fcc.gov/ecfs/search/search-filings/filing/111608400758; Brian Krebs, Hackers Claim They Breached T-Mobile More Than 100 Times in 2022, Krebs on Security (Feb. 28, 2023), https://krebsonsecurity.com/2023/02/hackers-claim-they-breached-t-mobile-more-than-100-times-in-2022/ (attributing more than 100 days of attacks in 2022 to cybercrime groups known to be active in and effective at SIM-swapping).

[83] Brian Krebs, Can We Stop Pretending SMS Is Secure Now?, Krebs on Security (Mar. 16, 2021), https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/.

communications would not be hindered by permitting survivors to effectuate a line separation. Indeed, the Commission seems to address these concerns already.[84]

Regarding the Commission's line separation authentication questions for survivors who are not primary account holders,[85] it is conceivable that an abuser uses an address the survivor is not aware of for their phone bills. Even if it is the same address as their residence, the survivor might not have access to the abuser's account number, PIN, or password. If an abuser has multiple phones, a survivor may not know the phone number designated as the primary account owner's.[86] For these reasons, we urge the Commission to permit survivors to name any other phone number on the group plan from which they request their phone number be separated, not specifically the primary account holder's phone number.

Regarding notification,[87] each survivor's safety plan[88] may be different. While it may be appropriate for the Commission to set minimum and maximum bounds for when to notify the alleged abuser, the safest outcome for survivors would be for this to be a case-by-case determination made by the survivor. If the Commission decides to impose a maximum period of time to delay the notification to the abuser, it should require the provider to alert the survivor that this deadline is approaching. Regardless of whether the notification trigger comes from the

---

[84] *See, e.g.*, NPRM at ¶ 97; id. at ¶ 104 (noting that covered provider should complete/maintain line separation and make record of complaint in case further evidence substantiates fraud allegation).
[85] Id. at ¶ 47.
[86] It is also conceivable that an abuser would only have shared a virtual number (e.g. Google Voice number) rather than the actual phone number with a survivor. A survivor should still be able to effectuate a line separation request using this virtual number.
[87] NRPM at ¶¶ 77-78.
[88] Safety Planning, NNEDV (July 2019), https://nnedv.org/resources-library/safety-planning/ ("Safety planning is an individualized plan to keep people safe….Safety planning should always be focused on the needs of each individual survivor, and should be dynamic/flexible").

survivor indicating that it is safe to notify the abuser or from the deadline being reached, the communications services provider should immediately notify the survivor once the notification to the abuser has been sent. We note that in several domestic violence court jurisdictions, a temporary protective order may be renewed every two weeks and propose two weeks as the default (but renewable) increment for telecommunications services providers to check in with a survivor about whether it is safe to notify the abuser of the line separation.

IV. The Commission Should Require All Involved Parties to Prioritize Data Minimization, and Require Carriers to Implement Data Security Best Practices When Data Retention is Necessary.

Requiring people to surrender privacy for other modes of safety and support is unacceptable,[89] and this is especially true for survivors of domestic violence. As a result, we support the Commission's proposals that safeguard survivor information by implementing data minimization and data security practices such as masking and encryption. As noted in our NOI comments, the best solution is to collect only what data is necessary to provide a service, to delete that data immediately after it is no longer necessary, to use data security best practices to protect data for the short duration that it must be retained, and to use methods like differential privacy to prevent reverse engineering underlying data from statistical reporting.[90]

---

[89] *See, e.g.,* Khiara Bridges, Poverty of Privacy Rights (discussion of this in the child welfare context in which poor mothers are forced to choose between invasive interrogations required to benefit from public benefits programs or risking child protective services taking their kids away on neglect allegations).

[90] EPIC et al. NOI Comments at 16 ("The best solution is not to collect sensitive data and PII in the first place and to retain such data only for as long as is absolutely necessary. However, if such data must be kept longer-term, the Commission might encourage use of secure storage protocols like encryption, or even obfuscation techniques that alter the data stored. In cases where statistics about the data must be made available—e.g., to researchers—the Commission might encourage use of differentially private querying techniques to further protect individual survivors.") (citing to EPIC Urges OSTP to Prioritize Differential Privacy (July 11, 2022), https://epic.org/epic-urges-ostp-to-prioritize-differential-privacy/).

For those reasons, we support the Commission's proposals to require disposal of survivor information not later than 90 days after receiving it, treating that data as confidential throughout its lifecycle, and applying the same requirements to vendors, contractors, etc. whom carriers task with handling this data.[91] We also support applying these requirements both to Customer Proprietary Network Information (CPNI) and to data that might not otherwise qualify as CPNI,[92] and support only permitting providers to use information submitted by survivors for processing the line separation request (e.g., not for any marketing purposes).[93]

The Commission asks about confidential treatment and secure disposal of data.[94] Regarding the technological aspects of the Commission's questions, we direct the Commission to EPIC's recent comments in the Commission's CPNI data breach docket[95] (as well as EPIC's comments to the FTC[96] and to the California Privacy Protection Agency[97]) in which we outline the near-consensus surrounding baseline data security practices. These would include access controls, secure password policies, traffic monitoring, internal firewalls, and other methods to

---

[91] NPRM at ¶ 53.
[92] Id. at ¶ 54.
[93] Id. at ¶¶ 55, 76.
[94] Id. at ¶ 55.
[95] *See In re* Data Breach Reporting Requirements, Reply Comments of EPIC, et al., WC Docket No. 22-21 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814 [hereinafter "EPIC et al. CPNI Breach Reporting Reply Comments"].
[96] *See* Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem, Comments of the Electronic Privacy Information Center to the Federal Trade Commission, R111004, at 194-216 (Nov. 2022), https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security/.
[97] *See* Comments of the Electronic Privacy Information Center, Center for Digital Democracy, and Consumer Federation of America, to the California Privacy Protection Agency, Proceeding No. 02-23, at 14-30 (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/. Id. at App. 2.

safeguard against unauthorized access to sensitive data.[98] Regarding the policy aspects of the Commission's confidentiality and security questions, we urge the Commission to clarify how its authorities under 222 and 201(b) support use of fines and other enforcement actions in response to breaches of survivor data.[99] We agree with each of the Commission's conclusions about its legal authority, but especially sources grounded in direction from Congress, Section 201(b), and "safety of life" under section 1.[100] We support the Commission's proposal to treat unauthorized disclosure of or access to information submitted by survivors as evidence that a provider did not treat information confidentially.[101] Moreover, where it is line separation request data that has been exposed, the Commission could bring enforcement actions for violations of its CPNI Rules (as this data was provided by the subscriber) and could conclude that a carrier who has exposed survivor data has imposed unjust or unreasonable practices in connection with a communication service. In addition to covering data exposed as a result of incomplete disposal[102] and data exposed through an insecure mechanism offered to survivors as a means of submitting line

---

[98] These data security practices are responsive to the Commission's inquiries in this NPRM insofar as they reflect best practices in data security, *see, e.g.*, NPRM at ¶ 55 (inquiring about restricting employee access, separate databases, encryption, etc.).
[99] EPIC et al. CPNI Breach Reporting Reply Comments at 5-11.
[100] NPRM at ¶ 146. Section 5(b)(3)(A)(ii) (directing the Commission to require providers to omit any records of calls or text messages to covered hotlines from customer-facing logs); 47 USC 201(b) (any "charge, practice, classification, or regulation [in connection with a communications services] that is unjust or unreasonable is declared to be unlawful…The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter"); 47 USC 151 (establishing the Federal Communications Commission in part "for the purpose of promoting safety of life and property through use of wire and radio communications").
[101] NPRM at ¶¶ 55, 60.
[102] Id. at ¶ 55.

separation requests,[103] these protections should also apply to any data that a provider has chosen to retain.[104]

The Commission asks how to safeguard survivor confidentiality while processing line separation and port requests if the survivor is also seeking to qualify for the designated program (e.g. Lifeline or ACP).[105] We disagree with the Commission that its definition of "customer" under its CPNI rules is limited only to those to whom the "carrier is currently providing service",[106] and note that at a minimum Lifeline applicant data is explicitly protected under the Commission's 222 and 201(b) privacy authorities.[107] EPIC et al. recently argued that any consumer who attempted to form a carrier-consumer relationship should be protected by the Commission's CPNI rules.[108] This is consistent with the STOP Violence Against Women Act (VAWA) protocols as well.[109] We urge the Commission to adopt a similar interpretation in this proceeding.

---

[103] Id. at ¶ 60.
[104] For example, survivor data that was obtained through the line separation request mechanism but exposed in a different database (i.e. arguably not covered by protections for breaches within the request mechanism) and exposed before the carrier initiated an attempt to dispose of the data securely (perhaps because it was within the 90-day window) should still be protected.
[105] NPRM at ¶ 96.
[106] Id. at ¶¶ 98-99.
[107] *See in re* TerraCom Inc. and YourTel America, Inc., Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1_Rcd.pdf.
[108] EPIC et al. CPNI Breach Reporting Reply Comments at 25-26.
[109] 34 USC §12291(b)(2)(B) (covering "information collected in connection with services requested, utilized, or denied through grantees' and subgrantees' programs, regardless of whether the information has been encoded, encrypted, hashed, or otherwise protected").

The Commission asks about best practices to prevent data leakage from abuser pretexters[110] claiming to be survivors in order to obtain survivor information such as their address.[111] We encourage the Commission to prohibit the disclosure of address information specifically because of the unique threat it could pose to survivors, even if the request appears to come through official channels.[112] More generally, requiring multiple factors to authenticate the individual could mitigate this problem—for example, relying on something the survivor has (such as a multi-factor authentication app registered to their separated phone number), not merely something they know (which their abuser might also know).[113] Survivors are vulnerable to various forms of tech-enabled abuse precisely because their abuser often knows information that can help bypass traditional cybersecurity measures.[114] The Commission's rules should reflect this reality.

We support the Commission's proposal to protect the privacy of alleged abusers.[115] We urge the Commission to treat the reason for line separation (i.e., alleged abuse) as CPNI for alleged abusers as well as for survivors. The Safe Connections Act prioritizes the safety and

---

[110] *See generally* in re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information, CC Docket No. 96-115; IP-Enabled Services, WC Docket No. 04-36, Report & Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (rel. April 2., 2007).
[111] NPRM at ¶ 178.
[112] Even disclosure to law enforcement can be problematic, see Section V below.
[113] "multi-factor authentication", National Institute of Standards and Technology, Computer Security Resource Center, https://csrc.nist.gov/glossary/term/multi_factor_authentication (last visited Apr. 10, 2023) ("authentication using two or more factors to achieve authentication"). However, it is also possible that an abuser would have access to the second device or email account used for multi-factor authentication.
[114] Karen Levy & Bruce Schneier, *Privacy Threats in Intimate Relationships*, 6 J. Cybersecurity 1 (2020), https://academic.oup.com/cybersecurity/article/6/1/tyaa006/5849222.
[115] NPRM at ¶ 179.

stability of the survivor, not actions against the alleged abuser. For this reason, and especially because we are advocating for self-attestation of survivor status rather than requiring certified proof of abuse, it would be inappropriate for a survivor's participation in the Commission's programs to have repercussions for the alleged abuser beyond phone line separation.

We agree with the Commission that protecting the privacy of calls and text messages to hotlines (and shelters) is in the public interest.[116] We support the Commission's proposal to establish penalties for failing to protect survivors by including calls to hotlines and shelters in phone bills.[117] In particularly egregious instances of violating its rules in this proceeding, the Commission could also threaten to reduce or terminate a communications service provider's federal funding; survivor services providers who fail to meet their requirements under VAWA and Victims of Crime Act (VOCA) are subject to such a requirement.[118]

We support the Commission's proposal to require USAC to establish a qualification number,[119] accept alias names,[120] and accept the address of a survivor support organization or

---

[116] Id. at ¶ 110.
[117] Id. at ¶ 144.
[118] Law Enforcement-Based Victim Services in Minnesota: Privacy, Privilege, and Confidentiality, National Crime Victim Law Institute 10 (Sept. 2021), https://ncvli.org/wp-content/uploads/2022/01/Minnesota-Privacy-Privilege-and-Confidentiality-last-updated-2021.pdf (describing confidentiality requirements); U.S. Department of Justice, DOJ Grants Financial Guide 12 (Mar. 2022), https://www.ojp.gov/sites/g/files/xyckuh241/files/media/document/DOJ_FinancialGuide_1.pdf (noting DOJ can withhold grant funds from programs that don't meet audit compliance); *see also* Leslye Orloff, VAWA Confidentiality, National Immigrant Women's Advocacy Project 4 (2015), https://niwaplibrary.wcl.american.edu/wp-content/uploads/2015/pdf/VAWA-Confidentiality-and-Breaches.pdf (officials who breach VAWA confidentiality can be disciplined and fined up to $5000 per breach).
[119] NPRM at ¶ 168.
[120] Id. at ¶ 165.

alias address[121] for survivors in order to minimize the amount of personal information survivors need to provide. For similar privacy and safety reasons, we also support the Commission's proposal to mask subscriber data in USAC systems.[122] We support the Commission's proposal to omit survivor enrollments from USAC reports.[123] Alternatively, we suggest the Commission direct USAC to implement differential privacy[124] to make it impossible to reverse engineer personal information from USAC's reports.

Regarding program evaluation, we encourage the Commission to limit initial communications with survivors to what is essential to ensure the survivor's safety, to ask questions to inform ongoing efforts after the initial eligibility period has ended, and to refrain from collecting PII at any point in the feedback and performance management process.[125]

V. The Commission Must Implement Safeguards to Protect Survivors from Misuse of Access to Their Data by Law Enforcement.

While the NPRM acknowledges that an abuser may fraudulently contact a call center to attempt to obtain information about the survivor they intend to victimize,[126] it fails to recognize

---

[121] Id. at ¶ 166.
[122] Id. at ¶ 178.
[123] Id. at ¶ 180.
[124] *See, e.g.*, EPIC Urges OSTP to Prioritize Differential Privacy, epic.org (July 11, 2022), https://epic.org/epic-urges-ostp-to-prioritize-differential-privacy/; EPIC Urges NIST to Emphasize Differential Privacy in Paper on De-Identifying Government Data Sets, epic.org (Jan. 17, 2023), https://epic.org/epic-urges-nist-to-emphasize-differential-privacy-in-paper-on-de-identifying-government-data-sets/. A 2019 study found that 99.98% of Americans could be correctly identified in any dataset using 15 demographic attributes. *See* Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, Nature (July 23, 2019), https://www.nature.com/articles/s41467-019-10933-3. An older study (2000) made similar findings with only three datapoints. *See* Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University, Data Privacy Working Paper 3 (2000), https://dataprivacylab.org/projects/identifiability/paper1.pdf.
[125] NPRM at ¶ 181.
[126] NPRM at ¶ 178.

the unfortunate reality of an abuser misusing law enforcement access to private data (either because they are an agent of the law or because they have connections to law enforcement staff).[127] We do not wish to frustrate the attempts of a survivor engaging law enforcement as a means of protecting themselves; however, the Commission cannot turn a blind eye to the well-documented history of law enforcement misuse of data access for personal purposes. We highlight a few examples in this section but include a non-exhaustive list of notable incidents in Appendix 2.

As we noted in our NOI comments, "abusers have connections within police departments; in some instances the abuser may be a law enforcement officer themself."[128] The Commission is itself well aware of how law enforcement agents may abuse their access to subscriber data (as in the instance of Sheriff Hutcheson's use of Securus to obtain location data on his predecessor, a judge, and at least five highway patrol officers).[129] While mechanisms may exist to address this misconduct after the fact,[130] whether those mechanisms are fully employed is at best uncertain and at worst unlikely.[131] Moreover, while initial prevention is preferable to

---

[127] Frascella and Olsen, *supra* note 24 ("abusers use various methods of surveillance and coercion to victimize survivors, and may have connections within law enforcement organizations (or may be law enforcement officers themselves)").
[128] EPIC et al. NOI Comments at 17-18 n 62-63; *see also* Leigh Goodmark, *Hands Up at Home: Militarized Masculinity and Police Officers Who Commit Intimate Partner Abuse*, 2015 BYU L. REV. 1183.
[129] *See, e.g.*, *In re* AT&T Inc., File No.: EB-TCD-18-00027704 at 40 (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf.
[130] These may be driven by bad press at least as much as by actual policy. Sadie Gurman, Across US, Police Officers Abuse Confidential Databases, Associated Press (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43.
[131] *See, e.g.*, Thomas Peele, Kensington Cops Used Confidential Database to Gather Information on Police Board Member, KQED (Feb. 20, 2019) ("only 54 of the over 1,000 officers found to

remediation after the fact in any case of law enforcement misconduct, the Commission has the opportunity in this rulemaking to *prevent domestic violence* facilitated by law enforcement access to survivor data. As such, we urge the Commission to clarify that when it describes situations in which "law enforcement needs access to [call and text message records],"[132] it means *at the request of a survivor*, assuming the survivor is still living.

We also urge the Commission to distinguish between lawful requests for information and unauthorized attempts to access survivor data by individuals who happen to be affiliated with a law enforcement organization (LEO). Unauthorized attempts by law enforcement agents to obtain survivor data occur outside the context of a criminal investigation and do not represent the actual needs of the LEO; as such, the Commission's mandates pertaining to law enforcement[133] should not inhibit the Commission's ability to prevent unauthorized attempts by law enforcement agents to obtain survivor data.

VI. The Commission Should Offer Carriers Guidance in Supporting Survivors with Device-Related Privacy and Safety Concerns.

We applaud the Commission for its attentiveness to on-device threats to survivor safety.[134] Stalkerware—phone apps that abusers can use as a tool for invasive monitoring of cell

---

have improperly access the database had charges filed against them"); Nicholas E. Mitchell, 2015 Annual Report, Denver Office of the Independent Monitor (2016) ("reprimands that are generally imposed on DPD officers who misuse the databases do not reflect the seriousness of that violation, and may not sufficiently deter future misuse").

[132] NPRM at ¶ 114.

[133] These mandates include to "consider the ability of law enforcement agencies or survivors to access a log of calls or texts messages in a criminal investigation or civil proceeding," id. at ¶ 111, and to make sure its rules omitting records from customer-facing logs do not "limit or otherwise affect the ability of a law enforcement agency to access a log of calls or text messages in a criminal investigation" nor "alter or otherwise expand provider requirements under the Communications Assistance for Law Enforcement Act," Safe Connections Act, § 5(b)(3)(C).

[134] NPRM at ¶ 104; id. at ¶ 130 (recognizing the limits of what removing call logs can achieve for survivor safety).

phone or tablet activity—are an increasingly pervasive attack vector favored by abusers.[135] Almost all 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.[136] There are numerous resources available to assist phone subscribers with detecting and removing stalkerware, some are not limited to technical considerations and also address the real-world harm that may result when an abuser discovers someone attempted to remove the stalkerware.[137] Because subscriber safety can be placed at risk[138] both by removing stalkerware (due to abuser learning of such removal) and by not removing stalkerware (due to continued abuser control over survivor), we urge the Commission to require providers to have some mechanism in place to assist survivors who specifically seek to detect and remove stalkerware on their devices. For example, when transferring the survivor's data from their old device to a new device, stalkerware may also be transferred (and therefore continue to surveil the survivor on

---

[135] *See, e.g.*, Eva Galperin, Stalkerware: 2021 in Review, Electronic Frontier Foundation (Dec. 25, 2021), https://www.eff.org/deeplinks/2021/12/stalkerware-2021-review ; Eva Galperin, Fighting Tech-Enabled Abuse: 2022 in Review, Electronic Frontier Foundation (Dec. 23, 2022), https://www.eff.org/deeplinks/2022/12/fighting-tech-enabled-abuse-2022-year-review; Brian X. Chen, 'Stalkerware' Apps Are Proliferating. Protect Yourself., New York Times (Sept. 29, 2021, updated Sept. 30, 2021), https://www.nytimes.com/2021/09/29/technology/personaltech/stalkerware-apps-protection.html; Zach Whittaker, Your Android phone could have stalkerware, here's how to remove it, TechCrunch (Feb. 22, 2022), https://techcrunch.com/2022/02/22/remove-android-spyware/.

[136] Frascella and Olsen, *supra* note 24 (referring to What is Stalkerware?, Safety Net Project, https://www.techsafety.org/spyware-and-stalkerware-phone-surveillance for further reading).

[137] *See* Whittaker, *supra* note 135; Stalkerware detection, removal and prevention, Coalition Against Stalkerware, https://stopstalkerware.org/information-for-survivors/ (last visited Apr. 10, 2023); Resources, Clinic to End Tech Abuse (CETA), https://www.ceta.tech.cornell.edu/resources (last visited Apr. 10, 2023); Technology Safety & Privacy: A Toolkit for Survivors, Safety Net Project, https://www.techsafety.org/resources-survivors (last visited Apr. 10, 2023).

[138] NPRM at ¶ 146 (addressing "safety of life").

their new device). To prevent this outcome, staff should be trained to treat that transfer differently. Also, although we believe consumer education materials should address the possibility of stalkerware, the Commission should avoid mandating policies that might result in additional unfounded anxiety for survivors, as false positives for stalkerware might cause. We believe the optimal solution is staff trained to support survivors, with clear instructions as to how to reach those staff members.

The Commission should also consider its authority to investigate the prevalence of stalkerware.[139] The Federal Trade Commission[140] and the New York Attorney General[141] have brought recent enforcement actions against purveyors of stalkerware (colloquially referred to as "spyware"), securing remedies such as outright bans, requirements that app developers ensure apps will only be used for legitimate purposes, and requirements that apps notify device owners that their devices are being monitored. Evidence of carriers being somehow involved in the creation, distribution, and/or promotion of stalkerware which collects or discloses CPNI would give the Commission a compelling basis to investigate stalkerware applications (and the potential

---

[139] Although we discuss stalkerware here in the context of phones turned into tracking devices, similar concerns apply to the detection and removal of Bluetooth-enabled devices designed expressly for tracking. *See, e.g.*, Andrew Crawford and Erica Olsen, Stopping Bluetooth Location Trackers From Becoming People Trackers, Tech Policy Press (Mar. 2, 2023), https://techpolicy.press/stopping-bluetooth-location-trackers-from-becoming-people-trackers/.

[140] FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data; *In re*: Retina-X Studios, LLC, https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3118-retina-x-studios-llc-matter (last updated Oct. 22, 2019).

[141] Press Release, Attorney General James Secures $410,000 from Tech Companies for Illegally Promoting Spyware and Violating New Yorkers' Privacy, Letitia James New York State Attorney General (Feb. 2, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-secures-410000-tech-companies-illegally-promoting-spyware.

harm to subscribers that they perpetuate),[142] though we do not concede that the Commission could not take action in other circumstances.

VII. The Commission Should Interpret "Hotline" Broadly in This Proceeding.

We support the Commission's implementation of a central database of hotlines to satisfy the requirements of the Safe Connections Act.[143] In particular, we support the Commission's proposal to include numbers that do not serve exclusively as hotlines in the central database, to interpret hotline as broadly as possible,[144] and to include texting-only hotline numbers.[145] The Commission should be clear that its interpretation of "hotline" is intended to apply to the obligations of telecom service providers in this rulemaking only and is not intended to impact the grant-based or other requirements of supportive services providers.

We support the Commission's proposal to update the central database on a monthly basis.[146] Regarding monitoring for new numbers to add to the central database,[147] the Commission could work with state supportive services organizations to ensure new organizations

---

[142] As Comm'r Starks noted of Securus in the NALs against the (then-four) major carriers. *See, e.g.*, *In re* AT&T Inc., File No.: EB-TCD-18-00027704 at 39 (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/FCC-20-26A1.pdf ("I recognize that uncovering this data would have required gathering information from the third parties on which the carriers' relied. But we should have done that via subpoenas if necessary. We had the power—and, given the length of this investigation, the time—to compel disclosures that would help us understand the true scope of the harm done to consumers."); id. at 42 ("There may be legal limitations on the Commission's ability to take enforcement against the company for its misuse of customer location data. But that is no excuse for failing to conduct a comprehensive investigation—including issuing subpoenas to Securus—of the events in question here. That information would have enriched our investigation and could have been provided to other agencies for investigation and enforcement.").
[143] NPRM at ¶¶ 109-10.
[144] Id. at ¶ 127.
[145] Id. at ¶ 116.
[146] Id. at ¶ 136.
[147] Id. at ¶ 138.

within the state are aware of the importance of submitting their contact information to the central database operator. We urge the Commission to permit individual hotline operators to submit multiple numbers, as the only consequence of having numbers listed is that they are hidden from call logs[148] (and if the Commission enacts its proposal, they will be listed publicly in the database).[149]

We agree with the Commission that survivor confusion might result from delays or exemptions from compliance,[150] and further note that if survivors are expecting updates to be implemented quickly, the failure to do so could result in not merely confusion but harm.[151]

VIII. Conclusion

We appreciate the opportunity to respond to the Commission's NPRM on supporting survivors of domestic violence.

Respectfully submitted, this the 12th day of April 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

Jessie
Safety Net Technology Safety Specialist
NNEDV

[148] Id. at ¶ 133.
[149] Id. at ¶ 134.
[150] Id. at ¶¶ 142, 115.
[151] Id. at ¶ 143.

APPENDIX 1

Descriptions and Interests of Filers

***Electronic Privacy Information Center*:** Electronic Privacy Information Center (EPIC) was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC encourages laws, regulations, and policies that safeguard user privacy and protect users from technology-facilitated abuse and harassment. *See, e.g.,* Comments of EPIC to Fed. Trade Comm'n, *Re:* Support King, LLC (SpyFone.com), No. 192 3003 (Oct. 8, 2021), available at https://epic.org/documents/in-the-matter-of-support-king-llc-spyfone-com/ ; Br. of Amici Curiae Electronic Privacy Information Center (EPIC) in Support of Appellant, Herrick v. Grindr, 765 Fed. Appx. 586 (2d Cir. 2019); Online Harassment, EPIC.org, https://epic.org/issues/democracy-free-speech/online-harassment/.

***National Network to End Domestic Violence*:** The National Network to End Domestic Violence (NNEDV), a social change organization, is dedicated to creating a social, political, and economic environment in which violence against women no longer exists. NNEDV is a leading voice for domestic violence survivors and their advocates. As a membership and advocacy organization of state and territorial domestic violence coalitions, allied organizations and supportive individuals, NNEDV works closely with its members to understand the ongoing and emerging needs of domestic violence victims and advocacy programs. NNEDV ensures survivors' needs are heard and understood by policymakers at the national level. NNEDV's Safety Net Project focuses on the intersection of technology and domestic and sexual violence and works to address how it impacts the safety, privacy, accessibility, and civil rights of victims.

Cyber Civil Rights Initiative: The Mission of the Cyber Civil Rights Initiative (CCRI) is to combat online abuses that threaten civil rights and civil liberties. CCRI's Vision is of a world in which law, policy and technology align to ensure the protection of civil rights and civil liberties for all.

Clinic to End Tech Abuse: The Clinic to End Tech Abuse (CETA) is a part of Cornell Tech, a campus of Cornell University located in New York City. Clinic volunteers are graduate students and professionals who have expertise in fields such as computer security, human-computer interaction, and computing for underserved communities. They receive special training on detecting technology-related abuse and working with people who have survived trauma. CETA provides its clinic services through a collaboration with the New York City Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV).

Electronic Frontier Foundation: The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world.

Iowa Coalition Against Domestic Violence: The Iowa Coalition Against Domestic Violence (ICADV) represents 21 local agencies providing direct services to crime victims. ICADV works with federal, state, and local policymakers and crime victim service providers throughout Iowa to advance public policies and provide effective support services to prevent violence, enhance victim safety, and support healing from trauma. Our service delivery model prioritizes supporting survivors in obtaining and maintaining economic security as the most effective path toward long-term stability, healing, and a violent free future. Our survivor-centered approach to victim services and policy advocacy seeks to center the voices and experiences of historically excluded survivors to advance safety for all.

National Coalition Against Domestic Violence: Our mission is to lead, mobilize and raise our voices to support efforts that demand a change of conditions that lead to domestic violence such as patriarchy, privilege, racism, sexism, and classism. We are dedicated to supporting survivors and holding offenders accountable and supporting advocates.

National Consumer Law Center® (NCLC®): Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law, telecommunications and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and utility publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness.

The National Domestic Violence Hotline: 24 hours a day, seven days a week, 365 days a year, the National Domestic Violence Hotline (The Hotline) provides essential tools and support to help survivors of domestic violence so they can live their lives free of abuse. The Hotline has answered over 6 million contacts, with services operated by expert advocates and other staff members dedicated to spreading education and awareness about domestic violence.

National Resource Center on Domestic Violence (NRCDV): Established in 1993, the National Resource Center on Domestic Violence ("NRCDV") is a national, non-profit organization that works to strengthen and transform program and community efforts to prevent and end domestic violence. This mission is accomplished through the promotion of equitable and effective public policy, engagement in prevention efforts, and provision of research, training, and technical assistance.

Ohio Domestic Violence Network: The Ohio Domestic Violence Network (ODVN) advances the principles that all people have the right to an oppression and violence-free life; fosters changes in our economic, social, and political systems; and brings leadership, expertise, and best practices to community programs. ODVN's purpose is to support and strengthen Ohio's response to domestic violence through training, public awareness, and technical assistance and to promote social change through the implementation of public policy.

Pennsylvania Coalition Against Domestic Violence (PCADV): The Pennsylvania Coalition Against Domestic Violence (PCADV) is a statewide collaborative membership organization committed to ending intimate partner violence and all forms of violence and oppression. Founded in 1976, PCADV is the oldest statewide domestic violence coalition in the nation. Each year, its network of 59 local domestic violence programs provides free and confidential direct services to nearly 90,000 victims and survivors of domestic violence and their children in all 67 counties of the Commonwealth. Together, local programs and the statewide Coalition work in collaboration to deliver a continuum of services, support, and systems to help victims and survivors find safety, obtain justice, and build lives free of abuse.

The Pennsylvania Utility Law Project (PULP): The Pennsylvania Utility Law Project (PULP) is a statewide specialty legal services project within the Pennsylvania Legal Aid Network. PULP's mission is to secure just and equitable access to safe and affordable energy, water, and telecommunication services for Pennsylvanians experiencing poverty. We work to achieve this mission by empowering individuals and communities through the provision of direct legal representation, advocacy, education, and support services. The ability of survivors of domestic violence to access safe, stable telecommunication services is of paramount importance, and critical to ensuring all Pennsylvanians have access to a safe and healthy home in a community where they can thrive.

Thomas Kadri: Thomas Kadri is an assistant professor at the University of Georgia School of Law, with affiliations in Women's Studies and Journalism & Mass Communication. He is also an affiliated researcher with the Clinic to End Tech Abuse at Cornell and serves on the board of directors for Project Safe, an Athens nonprofit working to tackle intimate partner violence. His work on digital privacy and abuse is supported by the National Science Foundation and appears in the *UCLA Law Review*, *Texas Law Review*, and *New York Times*. He received his Ph.D. from Yale Law School, J.D. from the University of Michigan, and M.A. from the University of St Andrews in Scotland.

APPENDIX 2

Personal Misuse of Data Access by Law Enforcement (Non-Exhaustive List)

General Commentary

1. Sadie Gurman, Across US, Police Officers Abuse Confidential Databases, Associated Press (Sept. 28, 2016), available at https://web.archive.org/web/20230119123143/https://apnews.com/article/699236946e3140659fff8a2362e16f43 (noting that it is impossible to know how many violations occur, that in many cases it is unclear whether any punishment was given at all, noting that in 2013 Minnesota changed the way officers access the state driver database after an audit revealed that over half of the 11,000 law enforcement personnel made searches that appeared questionable)
2. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Latent Effects of Computer-Based Record Keeping 19 (1973), available at https://www.justice.gov/opcl/docs/rec-com-rights.pdf ("most leakage of data from personal data systems, both automated and manual, appears to result from improper actions of employees either bribed to obtain information, or supplying it to outsiders under a 'buddy system' arrangement")

Specific Instances

3. Josh Wood, Feds: Ex Louisville Police Officer Used Law Enforcement Tech To Help Hack Sexually Explicit Photos From Women, LEO Weekly (Oct. 12, 2022), https://www.leoweekly.com/2022/10/feds-ex-louisville-police-officer-used-law-enforcement-tech-to-help-hack-sexually-explicit-photos-from-women/ (using law enforcement access to Accurint to obtain information about women which he would then share with a hacker to obtain sexually explicit photos and videos from the victims' Snapchat accounts which he would use to extort more images from his victims)
4. Joseph Cox, US Marshal Charged for Using Phone Location Tool to Track People He Knew, Vice (June 14, 2022), https://www.vice.com/en/article/k7bqew/us-marshal-securus-phone-location-tracked (US Marshal uploading fake documents to Securus that he claimed gave him authority to track physical location of people he had personal relationships with as well as their spouses)
5. Sam Stanton et al., Hundreds of California Police Misuse Law Enforcement Computer Databases, Investigation Shows, Sacramento Bee (Nov. 13, 2019), https://www.desertsun.com/story/news/2019/11/13/california-police-misuselaw-enforcement-databases-computers/2509747001/ (highlighting one of more than 1,000 California law enforcement agency workers in the last decade found to have misused sensitive databases that are supposed to be accessed for only legitimate investigative purposes, whose punishment amounted to a $150 fine, and noting only 54 of 1,002 officers found to have improperly access the database had charges filed against them)
6. Louise Matsakis, Minnesota Cop Awarded $585K After Colleagues Snooped on Her DMV Data, Wired (June 21, 2019) https://www.wired.com/story/minnesota-police-dmv-database-abuse/ (describing officer who abused access to driver's license database to snoop on thousands of people in Minnesota, mostly women)

7. Melanie Ehrenkranz, Cop Used Police Database to Creep on Over 100 Women, Investigation Finds, Gizmodo (Mar. 8, 2019), https://gizmodo.com/cop-uses-police-database-to-creep-on-over-100-women-in-1833156806 (department discovered officer had made "several hundred questionable database queries of women")
8. Thomas Peele, Kensington Cops Used Confidential Database to Gather Information on Police Board Member, KQED (Feb. 20, 2019), https://www.kqed.org/news/11727412/kensington-cops-used-confidential-database-to-gather-information-on-police-board-member (board member characterized improper access by multiple officers and subsequent traffic stop as harassment)
9. Nicholas E. Mitchell, 2015 Annual Report, Denver Office of the Independent Monitor (March 15, 2016), https://www.denvergov.org/content/dam/denvergov/Portals/374/documents/2015AnnualReport_OIM.pdf (25 officers who accessed law enforcement databases, including the National Crime Information Center (NCIC), for improper purposes such as stalking, none were prosecuted); at 10 ("reprimands that are generally imposed on DPD officers who misuse the databases do not reflect the seriousness of that violation, and may not sufficiently deter future misuse")
10. Dan Krauth and Mc Nelly Torres, Cops Use Tech to "Stalk" Exes, NBC6 (Nov. 18, 2014), https://www.nbcmiami.com/news/local/nbc-6-investigation-cops-use-tech-to-stalk-exes/61005/ (72% of 29 officers disciplined with mere verbal or written reprimands for delving into sensitive information of romantic interests, ex-spouses, co-workers, famous athletes, and high-profile personalities)
11. Alina Selyukh, NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog, Reuters (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-toolson-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927 (noting that at least a dozen NSA employees have used secret government surveillance tools to spy on current or former spouses and lovers over the last decade, a practice known as "LOVEINT")
12. Kim Zetter, Female Cop Gets $1 Million After Colleagues Trolled Database to Peek at Her Pic, Wired (Nov. 5, 2012), https://www.wired.com/2012/11/payout-for-cop-database-abuse/
13. Erik Gallant, Audit finds Mass. Police improperly search Tom Brady's records 968 times (May 7, 2009), MassLive, https://www.masslive.com/sports/2009/05/audit_finds_mass_police_improp.html
14. M.L. Elrick, Cops tap database to harass, intimidate, www.freep.com (July 31, 2001), available at https://web.archive.org/web/20011128034017/http:/www.freep.com/news/mich/lein31_20010731.htm (more than 90 Michigan police officers, dispatchers, federal agents, and security guards abused the Law Enforcement Information Network over a five-year period to access information about love interests, colleagues, bosses, or rivals)
15. Avis Thomas-Lester and Toni Lucy, Chief's Friend Accused of Extortion, Washington Post (Nov. 26, 1997), available at https://www.washingtonpost.com/wp-srv/local/longterm/library/dc/dcpolice/stories/stowe25.htm (DC police Lt. used law enforcement computer system to identify men visiting gay club through their license plates and subsequently attempted to extort them)