Before the

Federal Communications Commission

In the Matter of:

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

Further Notice of Proposed Rulemaking

Reply Comment of

Electronic Privacy Information Center (EPIC),

Clinic to End Tech Abuse at Cornell Tech (CETA),

National Network to End Domestic Violence (NNEDV), and

Public Knowledge

June 24, 2024

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

Table of Contents

I. Introduction

The **Electronic Privacy Information Center (EPIC),**[1] **the Clinic to End Tech Abuse (CETA),**[2] **the National Network to End Domestic Violence (NNEDV),**[3] and **Public Knowledge**[4] 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 continued implementation of the Safe Connections Act (hereinafter SCA or the Act), per the Further Notice of Proposed Rulemaking (FNPRM) published in the Federal Register on April 23, 2024.[5]

We file these comments to assist the Commission in prioritizing what it should include in an immediate Report and Order. We do not oppose the Commission including more than what is listed below (however this filing does not replace viewpoints articulated by signatories in prior filings), but we urge the Commission to, at a minimum, include the below. We do not comment on the authorities the Commission might use for our suggestions below, as that has already been outlined extensively in the record.[6]

The Commission should take into consideration that a survivor may be seeking to make use of proposed protections and supportive services in between attempts to escape their abuser.[7] We also note that where processes may amount to a race between counterclaims, the abuser is more likely to win that race, as they are often actively seeking to discover and exploit methods of control whereas a survivor is more often responding to the attempt at control only after it has already occurred. These types of scenarios have been discussed in the record,[8] but the

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

[2] The Clinic to End Tech Abuse (CETA) provides digital privacy and cyber security services to survivors of domestic violence experiencing technology-facilitated abuse. CETA has served over 700 survivors since it began operating in 2018, in partnership with the New York City Mayor's Office to End Domestic and Gender-Based Violence.

[3] The National Network to End Domestic Violence (NNEDV) represents the 56 state and U.S. territorial domestic violence coalitions, their nearly 2,000 member programs, and the millions of survivors they serve and advocate on behalf of each year.

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

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

[6] *See, e.g.*, Comment of EPIC and Public Knowledge, *In re* Supporting Suvivors of Domestic Violence FNPRM, WC Dkt. No. 22-238 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105242630421222 [hereinafter "EPIC PK FNPRM Comment"]; Comment of Free Press, *In re* Supporting Suvivors of Domestic Violence FNPRM, WC Dkt. No. 22-238 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105231287424285.

[7] *See, e.g.*, EPIC PK FNPRM Comment at 10; Comment of EPIC, et al., *In re* Supporting Survivors of Domestic and Sexual Violence, WC Dkt. No. 22-238 at 10 n. 55 (Apr. 12, 2023), available at https://epic.org/documents/in-the-matter-of-supporting-survivors-of-domestic-and-sexual-violence-nprm/#_ftn55 [hereinafter "EPIC NNEDV et al NPRM Comment"].

[8] *See, e.g.*, Comment of EPIC, et al., *In re* Supporting Survivors of Domestic and Sexual Violence at Section III(d) (Aug. 18, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/1081899226693, available at https://epic.org/documents/in-the-matter-of-supporting-survivors-of-domestic-and-sexual-violence/#d-the-

Commission might convene experts and other stakeholders to offer walkthroughs if it feels it does not adequately understand these dynamics.

Our joint recommendations are broken out into four Sections:

- In Section II, we urge the Commission to prioritize solutions that make services more accessible and useful to survivors in an immediate Report and Order.
- In Section III, we urge the Commission to prioritize solutions that mandate anti-abusability design for connected devices in an immediate Report and Order, highlighting examples already offered in the context of connected car services.
- In Section IV, we urge the Commission to undertake further inquiries to support survivors, suggesting what directions those inquiries should initially take.
- In Section V, although the Commission has adequate existing authority without the need for additional authorization from Congress, we respond to the Alliance for Automotive Innovation's (AAI's) model bill language.

The below suggestions are consistent with the five core principles we urge the Commission to keep in mind throughout this proceeding and any related proceedings.[9]

We thank the Commission and the Wireline Competition Bureau for their continued and timely attention to the needs of and challenges faced by survivors of domestic violence.

II. The Commission should prioritize solutions that make services more accessible and useful to survivors.

The Commission should promote access and utility of supportive services to survivors. This includes but is not necessarily limited to: enforcing compliance with verified subpoenas, requiring providers to accept redacted restraining orders, requiring providers to accept requests from authorized agents and advocates, requiring providers to honor deletion requests regardless of state of residence, and requiring providers to have 24/7 staff trained in trauma-informed and privacy-aware approaches to support survivors. While all of the suggestions in this section of our joint Reply Comments happen to be non-technological, the Commission may also consider technological solutions that make services more accessible and useful to survivors, for example implementing a web portal to accept requests from survivors (but see Section III(e) *infra*).

a. Enforcing compliance with verified subpoenas.

Multiple commenters observed that car manufacturers "frequently flout even legal subpoenas" about access information to smart car applications, for example in response to a

commission-should-bear-in-mind-the-realities-of-being-a-target-of-domestic-violence-when-considering-removing-participants-from-its-programming.

[9] *See* Coalition Comments of Electronic Privacy Information Center (EPIC) et al., WC Docket No. 22-238 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10524769628431 [hereinafter "Coalition FNPRM Comment"].

survivor seeking to demonstrate an abuser's defiance of a restraining order.[10] While it is important to protect user privacy, where lawful process has been followed,[11] providers should equip survivors with the evidence needed to effectuate legal protections.

We urge the Commission to require that companies verify the legitimacy of any seemingly lawful orders, as even court orders have been faked in the past.[12] Where an order is confirmed as valid (for example by contacting the issuing court, law enforcement organization,[13] or attorney), the connected car service provider should comply with it in a timely manner.

b. Requiring providers to accept redacted restraining orders.

Due to the nature of the personal information contained in a restraining order, and the absence of any need for the connected car service providers to have any information about the survivor beyond their status as such, the Commission should require providers to accept redacted restraining orders.[14] The concerns animating the need for documentation to prove survivor status, such as a restraining order, pertain to ensuring only survivors benefit from survivor-specific protections, such as line separation.[15] These concerns do not extend to the details of why the survivor seeks relief, indeed the Commission has noted that providers neither want to be in the position to make determinations about survivor status nor are qualified to make such determinations, beyond the very basics of indicia of fraud.[16] Where a survivor has already gone

[10] *See* Comment of CETA, Madison Tech Clinic at the University of Wisconsin-Madison, WC Docket No. 22-238 at 5-6 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105241552112348 ("survivors may need to know whether a perpetrator has accessed a smart car application in defiance of a restraining order; access logs as proof of stalking") [hereinafter "CETA MTC Comment"]; Comment of Privacy4Cars, the Plunk Foundation, Electronic Frontier Foundation, WC 22-238 at 15-17 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105240599325382 (example in which Tesla refused to comply with subpoena).

[11] The Commission has noted that it would not require a judicial order or grand jury subpoena for law enforcement to request information about survivors requesting a line separation, despite the risks of abuse of administrative subpoenas, due to the constraints of the Safe Connections Act. *See* Report and Order, *In Re*: Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform Modernization, Affordability Connectivity Program, WC Docket Nos. 22-238, 11-42, 21-450 at ¶ 216 (Rel. Nov. 16, 2023), https://docs.fcc.gov/public/attachments/FCC-23-96A1.pdf [hereinafter "R&O"].

[12] *See, e.g.*, EPIC PK FNPRM Comment at fn. 52; Joseph Cox, Hackers Are Selling Hacked Police Emails to Try to Grab Personal Data from Tiktok, Facebook (Aug. 31, 2023), https://www.404media.co/buying-and-selling-hacked-government-emails-edrs-discord-snapchat-facebook-tiktok/; *DEA Investigating Breach of Law Enforcement Data Portal*, Krebs on Security (May 12, 2022), https://krebsonsecurity.com/2022/05/dea-investigating-breach-of-law-enforcement-data-portal/ (noting in the context of a DOJ database being hacked that "when hackers can plunder 16 law enforcement databases, arbitrarily send out law enforcement alerts for specific people or vehicles, or potentially disrupt ongoing law enforcement operations — all because someone stole, found or bought a username and password — it's time for drastic measures."); *Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"*, KrebsonSecurity (Mar. 29, 2022), https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/.

[13] We note contacting the requesting officer may not be an adequate safeguard. *See* EPIC NNEDV et al. NPRM Comments at App'x 2, PDF pgs 39-40/40.

[14] *See* Comment of Privacy4Cars et al. at 20; Comment of National Network to End Domestic Violence (NNEDV), National Domestic Violence Hotline (NDVH), WC 22-238 at 5 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10523900520611 [hereinafter "NNEDV NDVH FNPRM Comment"].

[15] *See* R&O at ¶ 35.

[16] *See* R&O at ¶ 34.

through the process to obtain a restraining order and to redact sensitive information from that order, a provider should not then require the survivor to submit a wholly unredacted version of the order.

c. Requiring providers to accept requests from authorized agents and advocates.

Numerous commenters noted the benefit to survivors of permitting authorized agents and advocates to submit requests on their behalf.[17] As noted at several stages throughout this proceeding, there are many reasons why a survivor may choose to engage one service provider rather than another, and the Commission should not prescribe a single method by which survivors can obtain support.[18] We note that submitting requests on behalf of a survivor is a separate issue from attestating to survivor status, but re-iterate here our exhortation that the Commission interpret "victim services provider" broadly.[19]

d. Requiring providers to honor deletion requests regardless of state of residence.

As several commenters have noted, while some states have laws that require companies to honor deletion requests, there is no comprehensive federal privacy law, and so that leaves survivors in some states without an easy method to protect themselves by deleting data collected about them.[20] The Commission should require providers to honor deletion requests regardless of the survivor's state of residence. This should not be limited to instances in which a survivor may have relocated to another state to ensure their safety and subsequently sent a request for their data to be deleted based on the laws in their prior state of residence.

e. Requiring providers to have staff trained in trauma-informed and privacy-aware approaches, available 24/7 to support survivors.

The Commission should maximize the methods by which a survivor can obtain support; this includes 24/7 trained staff, as abusers do not wait until normal business hours to threaten the safety of their intended victims.[21] The National Network to End Domestic Violence (NNEDV) and The National Domestic Violence Hotline noted several reasons why customer service representatives may be ill-equipped to support survivors, absent appropriate training.[22] They also cited to the safety concerns implicit in forcing survivors to navigate multiple layers of escalation for customer service cases before reaching a resolution.[23] As Privacy4Cars, the Plunk Foundation, and Electronic Frontier Foundation noted, this hotline should be available 24/7, and should be staffed by representatives who can assist survivors with requests such as answering questions about connectivity, disabling location tracking, deactivating mobile app accounts, and

---

[17] *See, e.g.*, Comment of Privacy4Cars et al. at 20-21, 26, 33 (accept requests initiated by authorized agents and advocates); NNEDV NDVH FNPRM Comment at 5 (Broadband providers should accept authorization forms from third-party advocates); Comment of Free Press, WC 22-238 at 9 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105231287424285 (allow individuals to demonstrate survivor status through various care providers or self-attestation).

[18] *See, e.g.*, R&O at ¶ 52; EPIC PK FNPRM Comment at 2.

[19] *See* EPIC PK FNPRM Comment at 13.

[20] *See* Comment of Privacy4Cars et al. at 17; NNEDV NDVH FNPRM Comment at 1.

[21] *See* Comment of Privacy4Cars et al. at 8; NNEDV NDVH FNPRM Comment at 3.

[22] *See* NNEDV NDVH FNPRM Comment at 2-3.

[23] *See* id. at 2.

deleting data stored locally and remotely.[24] Where resources are provided to survivors, these should be written at an 8th grade level,[25] offered in every language the company markets in,[26] and additionally in some of the most common languages in the covered area.[27]

III. The Commission should prioritize solutions that mandate anti-abusability design for connected cars.

The Commission should prioritize solutions that mandate anti-abusability design for connected cars in an immediate Report and Order. We briefly offer a few suggestions below for where the Commission might start, based on what has already been filed in this docket. We note that these protections should not require proof of survivor status, not even at the level of self-attestation. These suggestions, which emphasize user safety and autonomy, include: physical proximity overrides (e.g. a user should be able to perform a factory reset), account security interfaces, data minimization and data security by default, persistent visual notification of data collection and data sharing, and a web portal or dial-in number that is easy to navigate and used for multiple purposes unrelated to support for domestic violence survivors.

The Commission should continue to work with stakeholders to develop an anti-abusable framework for connected devices,[28] which puts the onus on providers to make the services readily accessible (if not enabled by default outright), rather than putting a burden on survivors to be aware of, to understand, and to effectively maintain that functionality.[29] Additional solutions not detailed below might include: an automated factory reset or ease-to-effectuate right to reset,[30] multiple user accounts with no visibility into another's account,[31] mutually exclusive control,[32] granular user controls,[33] and audit logs.[34]

a. Requiring physical proximity overrides.

Users should be able to promptly delete data, to mitigate the harm when abusers obtain access to data and generally to protect the sensitivity of each user's location data. We have been encouraged by Chairwoman Rosenworcel's continued emphasis on the sensitivity of location data both in this proceeding and elsewhere.[35] Given the obvious risk to immediate physical safety, as well as more long-term concerns about inferences that can be made from historical

[24] *See* Comment of Privacy4Cars et al. at 8.
[25] *See* NNEDV NDVH FNPRM Comment at 7.
[26] *See* R&O at ¶ 46.
[27] *See* Comment of Free Press at 9-10.
[28] *See* NNEDV NDVH FNPRM Comment at 1; EPIC PK FNPRM Comment at 11-12.
[29] *See, e.g.*, EPIC PK FNPRM Comment at 8-9.
[30] *See* Comment of Privacy4Cars et al. at 14-15, 29-30, 32-33; CETA MTC Comment at 4.
[31] *See* CETA MTC Comment at 4.
[32] *See* id.
[33] *See* EPIC PK FNPRM Comment at 8.
[34] *See* id. at 14.
[35] *See, e.g.*, Press Release, Chairwoman Rosenworcel Probes Top Mobile Carriers on Data Privacy Practices (July19, 2022), https://docs.fcc.gov/public/attachments/DOC-385446A1.pdf; Press Release, Chair Rosenworcel Shares Mobile Carrier Responses to Data Privacy Probe and Announces Next Steps (Aug. 25, 2022), https://docs.fcc.gov/public/attachments/DOC-386596A1.pdf; Rosenworcel Statement, FCC Fines Verizon $46M for Location Data Violations, FCC-24-41 (Apr. 29, 2024), https://www.fcc.gov/document/fcc-fines-verizon-46m-location-data-violations/rosenworcel-statement.

data, the Commission should require that any connected car service provide each driver with the ability to disable location tracking on vehicles through functionality such as a factory reset mode.[36]

b. Requiring an account security interface.

We strongly support the proposals for transparency and isolation as anti-abusability design features advanced in CETA and Madison Tech Clinic's comment, specifically in the context of an account security interface that is readily-accessible to any user.[37] As they note in their comment, this should not include any information on the behavior of any other user's account (e.g. not include last login, or device name or type) but merely note how many other accounts there are that have access to the connected car service and what privileges each account has (e.g. can a given account remotely unlock doors, view real-time location information, view historical location information, etc.).[38] In at least one example, a survivor holding the title to the vehicle was not even able to determine whether their abuser had access to the vehicle or associated data. This is unacceptable.

c. Requiring data minimization and data security by default.

The Commission should require practices that ensure data minimization and data security by default, to protect survivors from some of the most obvious mechanisms by which their data might be inappropriate accessed and subsequently used to control, surveil, harass, or otherwise re-victimize them. This includes automatically deleting location data, making data inaccessible to users from other accounts, and periodic and randomized renewals for consent. This also includes strict limitations on the transmission and use of data, as well as encryption of transmitted data.

Location data for which no additional, affirmative step was taken to save it (e.g. marking it as Home or Favorite) should be deleted after a predetermined period of time. Distinct from subsection III(a) *infra* which requires a user to proactively take an action to delete data, this would be an automated process. Relatedly, where a car collects data under different user accounts, data should not be accessible across accounts (i.e., User B should not be able to access User A's data).[39]

There should be periodic renewed requests for consent at randomized intervals, to ensure one-time consent is not established by an abuser without the awareness of, control of, or ability to revoke consent by the survivor.[40] The Commission may need to convene stakeholders to determine the safest and most effective way to display these consent prompts to a driver.[41]

[36] *See, e.g.*, CETA MTC Comment at 4 (discussing "physical proximity overrides" and "exclusive control" as anti-abusable design); NNEDV NDVH FNPRM Comment at 3-4; Comment of Free Press at 4-5.
[37] *See* CETA MTC Comment at 4.
[38] *See* id.
[39] *See* id.
[40] *See* EPIC PK FNPRM Comment at 6-8; NNEDV NDVH FNPRM Comment at 2.
[41] *See* NNEDV NDVH FNPRM Comment at 1; EPIC PK FNPRM Comment at 11-12.

Data should not be transmitted outside the car unless strictly necessary.[42] Where it is strictly necessary to transmit data, that data should be encrypted and it should not be used except and exclusively for the purposes that made its transmission strictly necessary.[43]

We note that where a line separation is not involved, the Commission need not rely upon its authority under the Safe Connections Act. We also note that concerns about limiting access to data pertaining to other users of a shared device or account[44] are concerns of a different kind than concerns about limiting access to a physical device.

d. Requiring persistent visual notification of data collection and data sharing, such as location tracking.

The Commission should require both persistent and ad-hoc alerts to protect drivers from otherwise undisclosed surveillance. Connected car service providers, including vehicle manufacturers, should be required to create an obvious and persistent visual cue that informs individuals that their location is being tracked.[45] Additionally, providers should issue real-time alerts to drivers each time an account holder checks the location of the driver or of the vehicle.[46] As noted in Section III(a) *supra*, this should be accompanied by a simple process to disable location tracking and remote control.[47]

e. Requiring that a web portal or dial-in number for requesting survivor-specific services be easy to navigate and be used for multiple purposes.

The methods by which survivors reach out for support should be easy to understand (e.g. no manipulative design).[48] Additionally, providers should be mindful not to have a URL title that could expose survivors to greater risk of harm, ideally by combining multiple purposes into the single number, web portal, etc. so that it is not immediately obvious to an abuser that their intended victim was seeking support related to domestic violence (e.g. if the abuser views their browser history).[49]

IV. The Commission should undertake further inquiries into practices that pose heightened risks to survivors.

The Commission should investigate other practices that pose heightened risks to domestic violence survivors. Such inquiries would include aftermarket GPS or telematics equipment; the

[42] *See* Coalition FNPRM Comment at 2.

[43] *See* id. at 2-3.

[44] *See, e.g.*, section II(b) *supra* for how to share data about other users on a shared device in a privacy-protective way.

[45] *See* Comment of Privacy4Cars et al. at 12-13 (noting this will be required in California, that alert system could help in real-time).

[46] *See* NNEDV NDVH FNPRM Comment at 5.

[47] *See* Comment of Privacy4Cars et al. at 18-20.

[48] *See* id. at 19 (Require manufacturers to offer clear information for how survivors can protect themselves on a webpage); NNEDV NDVH FNPRM Comment at 5 (being mindful not to have a URL title that could expose survivors to greater risk of harm).

[49] *See* Comment of Privacy4Cars et al. at 8.

record suggests users are unable to disable these presently.[50] Inquiries would also include requiring a factory reset after rental periods, to reduce the likelihood of an abuser or stalker exploiting devices still-connected to the rental vehicle, and associated data.[51] These inquiries should also include location tracker discoverability (e.g. 4G LTE trackers), which we further note is not limited to the context of connected car services, and which tech clinics have indicated limited ability to assist survivors with absent action from the Commission.[52]

V. We offer responses to the model bill language proposed by the Alliance for Automotive Innovation (AAI), noting that the Commission presently has adequate authority to protect survivors from misuse of communications systems.

The Commission has adequate existing authority to implement many of the changes proposed in the docket; no additional authorization is required from Congress, although the Commission might seek cooperation from other federal agencies. Despite the fact that the Commission does not need additional Congressional authority, we offer the following recommended changes to the AAI's model bill language:[53]

- Advocates should be allowed to submit a request on behalf of a survivor.[54] Our reasoning for this appears above[55] and is well-documented in the record.
- The mandatory response time should be shorter than five days, but should allow some time for the company to verify the request.[56] This is to balance the urgency of complying with a survivor's request against the risk of an abuser attempting to leverage the request process to exert control over a survivor.[57] Two business days would likely satisfy this balance.
- We are opposed to preemption to the extent that the model bill would preempt more protective state or local laws or ordinances. This aligns with the text of the Safe Connections Act and the reasoning of the Commission.[58]
- The bill should require a minimum and a maximum lead time between (1) when a provider informs a survivor of when they will notify the abuser and (2) when that notification time actually occurs. For example, the bill requiring a minimum lead time of 24 hours would mean a provider would be prohibited from informing a survivor on 10am ET Monday morning that the provider will notify the abuser on Monday afternoon—the

[50] *See* id. at 29.

[51] *See* id. at 29-30.

[52] *See* CETA MTC Comment at 5. EPIC re-iterates that dual-use apps also fall into the category of technology that poses enhanced risk to survivors and which tech clinics cannot readily support survivors absent action from the Commission. Reply Comment of EPIC et al., *In re* Supporting Survivors of Domestic and Sexual Violence at 5-8 (May 12, 2023), available at https://epic.org/documents/reply-comments-in-re-supporting-survivors-of-domestic-and-sexual-violence-nprm/#a-the-commission-should-investigate-family-tracker-apps-and-similar-apps.

[53] *See* Comment of Alliance for Automotive Innovation, Attachment A, pg 17/22 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105230124421118.

[54] *See* NNEDV NDVH FNPRM Comment at 2, 4; Comment of Privacy4Cars et al. Exh B at 15.

[55] *See* Section II(c) *supra*.

[56] *See* NNEDV NDVH FNPRM Comment at 8; Comment of Privacy4Cars et al. Exh B at 15.

[57] *See, e.g.*, Section I, Section II(a) *supra*.

[58] *See, e.g.*, R&O at ¶ 101 fn. 405 (citing to 47 U.S.C. § 345(c)(3) ("This subsection shall not affect any law or regulation of a State providing communications protections for survivors (or any similar category of individuals) that has less stringent requirements for providing evidence of a covered act (or any similar category of conduct) than this subsection.").

notification to the abuser would have to occur on Tuesday morning at 10am ET or later. A maximum lead time is necessary to ensure timely relief to the survivor. The provider should still provide an accurate estimate of when the notification will occur. To keep with the same example, the provider should not indicate to the survivor that the abuser will be notified on Tuesday and then notify the abuser on Thursday, even if that would technically fall within the maximum lead time parameters of the bill.

We also note that the bill seems to limit its scope to apps "designed to be operated on a mobile device" which may exclude web-based services which can be accessed via a non-mobile device, for example via a desktop computer. We do not comment on the Commission's authority in this context but note that it would be beneficial to survivors to be able to obtain relief through whatever method is most convenient to them, regardless of the underlying technology.[59]

We thank the AAI for providing bill language that facilitates these kinds of conversations.

VI. Conclusion

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

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

[59] *See* EPIC PK FNPRM Comment at 11, 15-17.