COMMENTS OF A COALITION OF CIVIL SOCIETY GROUPS

to the

Federal Communications Commission

on

FNPRM Supporting Survivors of Domestic and Sexual Violence

89 Fed. Reg. 30303, WC Docket No. 22-238

May 23, 2023

Coalition Comment of Civil Society Groups:

The undersigned domestic violence survivor advocacy, privacy, government accountability, civil liberties, civil rights, racial justice, human rights, and other civil society groups submit this comment to urge the Federal Communication Commission (FCC, or "Commission") to foreground the needs of survivors of domestic and sexual violence and to protect privacy when regulating connected cars and other internet-connected devices. While many of the undersigned groups have submitted more detailed comments separately, we write here to emphasize the high-level principles that the FCC should follow to appropriately protect survivors and honor individuals' autonomy and agency in difficult situations.

Complex internet-connected devices like cars are creating novel avenues for abusers to stalk, monitor, and retain control over survivors. Car companies, wireless service providers, and third-party device sellers have rapidly rolled out new and interconnected monitoring features. We broadly refer to the networks of cars, cellphones/apps, third-party devices, and data storage by wireless providers and car companies as "connected car systems." These same companies have often done little, if anything, to provide users with sufficient autonomy to prevent stalking and other forms of remote monitoring. Cars meanwhile are vital and difficult to replace tools for survivors to ensure their physical safety and freedom. Survivors should not have to choose between maintaining privacy and security from an abuser and access to personal transportation. People should not have to abandon their cars to escape domestic violence.

Connected car systems are often both insufficiently private for individual drivers and unnecessarily leaky, as cars often send data to parties other than the driver/owner without the driver's consent. Many connected car systems fail to provide easy means for drivers to separate their connected car accounts or shield their data from a shared account potentially controlled by an abuser. Connected car systems also often fail to minimize data collection and data transmission, causing systems to leak data to automakers, wireless providers, and data brokers.

Detailed driving data from connected cars has ended up in the hands of insurance companies, major data brokers like LexisNexis, and become exposed in massive car company data breaches.

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

System design can substantially impact how easy it is for individuals to decide when and how information from a connected car will be transmitted beyond the car or the individual's account. Each user, and not only account owners, should be able to limit the data collected by connected car systems and decide who besides that user is allowed access to that data. Systems should provide plainly worded explanations of what data is collected and who it is sent to and give users an easy means for limiting that collection and transmission. Providing agency to individual users can allow people experiencing domestic violence to decide in the moment how to keep themselves safe. User-level agency recognizes that circumstances may change quickly in domestic violence scenarios, and that survivors themselves are best positioned to know their individual needs.

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

Safe Connections Act programs should be designed to require low bars for access. While covered providers might need to validate an individual user's identity, any purported need to verify their status as a survivor of domestic violence is outweighed by the clear burdens that would impose on survivors. Any additional validation beyond identity verification makes it harder for survivors to access needed services, could put them at heightened risk, and will have little if any ancillary benefits. Safe Connections Act programs for cars are targeted at a discrete population, and they are likely to provide relatively little incentive for non-survivors to utilize them. Many survivors may not have documents to validate their status, like a police report, restraining order, or divorce paperwork. Obtaining such documents may even be dangerous for them. Every survivor may go through a unique process separating from their abuser. With these concerns in mind, the Commission should collaborate with privacy and domestic violence experts in the implementation process to identify the documentation requirements that will result in the least burden on survivors, while also minimizing opportunities for abuse and fraud.

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

Dedicated survivor services are not enough to prevent all the harms caused by connected cars. Implementing data minimization and security requirements by default can help ensure that abusers do not get access to sensitive data like location data. A few principles can help ensure that connected car services are a benefit to survivors, not a source of harm. Generally, data and especially location data should only be collected for a discrete purpose. For example, location data for a GPS navigation system should only be collected when the system is in use. Data should also be stored on the car, not transmitted beyond the car unless necessary. On-car data should be regularly deleted by default and should be easy for drivers to delete manually if necessary. Further, all data should be encrypted and accessible only to authorized users, not to wireless providers or car companies beyond what is strictly necessary to provide their services.

Finally, when a connected car has multiple drivers with multiple accounts, by default car-related data should be accessible only to the driver who created that data.

Connected car systems should proactively prevent misuse.

The FCC should act to prevent further incidents of domestic violence by empowering survivors to get free from the control of their abusers; this means creating accessible mechanisms by which any user can restrict data collection and sharing. This also means rethinking assumptions about cybersecurity and user experience. For example, sending immediate notifications to vehicle owners when location data is disabled can have predictably dire safety implications where the owner is a would-be abuser. Similarly, companies fail to recognize how dangerous historical location data can be in the hands of a would-be abuser. To the extent that industry members have engaged, the connected car industry has focused on abuser access to real-time vehicle location data. Historical location data can be used to infer likely future locations or determine that an intended victim visited a shelter or other service provider in the past, possibly triggering violent retaliation. Connected car systems should proactively prevent these scenarios from occurring by design. Privacy by design is especially important because many survivors never seek services, including those who have been marginalized in other ways.

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

Survivors should not have to navigate complex bureaucratic systems to find out if services exist, and they should not need to jump through unnecessary hoops to qualify for those services. Car companies and wireless services providers should bear the burden of creating, implementing, and providing notice of survivor services programs. As noted above, these companies should incorporate privacy and security considerations into their design processes by default, with consideration to the particular needs of domestic violence survivors. Furthermore, as companies develop and implement specific programs for survivors, they should bear the burden of ensuring that survivors and the public are aware of these services. Companies should prioritize the safety and well-being of individuals who are subject to novel forms of monitoring and abuse because of connected car systems.

We therefore urge the FCC to implement the above recommendations. For any questions about the submission, please contact Chris Frascella, EPIC Counsel at frascella@epic.org.

Sincerely,

Center for Democracy & Technology
Communications Workers of America (CWA)
Cyber Civil Rights Initiative
DC Coalition Against Domestic Violence
Electronic Privacy Information Center (EPIC)
Fight for the Future
(list continues on next page)

Girl Security
Government Information Watch
Iowa Coalition Against Domestic Violence
Jewish Women International
Legal Momentum
National Consumer Law Center, on behalf of its low-income clients
The National Domestic Violence Hotline
National Network to End Domestic Violence
New America's Open Technology Institute
Pennsylvania Coalition Against Domestic Violence
Pennsylvania Utility Law Project (PULP)
Public Knowledge
Restore the Fourth
Surveillance Technology Oversight Project
UltraViolet