epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Statement of Alan Butler

Executive Director, Electronic Privacy Information Center (EPIC)

Hearing on "Breach of Trust: Surveillance in Private Spaces"

Before the

Subcommittee on Cybersecurity, Information Technology, and Government Innovation of the

Committee on Oversight and Government Reform

United States House of Representatives

May 20, 2025

Subcommittee Chair Mace, Ranking Member Brown, Committee Chair Comer, Ranking Member Connolly, and Members of Subcommittee, thank you for the opportunity to testify today on the threats we face from evolving technologies that facilitate *Surveillance in Private Spaces*. My name is Alan Butler, and I am Executive Director at the Electronic Privacy Information Center. EPIC is an independent nonprofit research organization established in 1994 to secure the right to privacy in the digital age for all people.

This hearing addresses a question that has been a central focus of modern privacy law since it was first developed more than a century ago—how can the law preserve our right to be let alone in response to technological developments that make intrusion, monitoring, coercion, and abuse easier and less expensive?

The stakes are high, and those of us working to advance policies and practices that can protect victims against abuse and provide meaningful guardrails on these powerful new technologies should focus on developing and promoting rules and standards that can help to prevent and mitigate these harms. In my testimony today, I will give a brief overview of how technological and cultural developments have shaped the course of modern privacy law over the last century. Then I will provide additional background on the unique bystander risks posed by connected devices and identify transparency and design standards that could help to mitigate these risks. Then I will briefly summarize some of the relevant legal standards concerning recording in semi-public and other shared spaces. And finally, I will offer a few thoughts on where future investigations could shed light on tech-enabled abuse and identify potential interventions.

1. **Technological advances in surveillance capabilities and the cultural shifts that have moved in tandem with those changes have guided the development of modern privacy law over the last century.**

When Samuel Warren and (soon to be) Justice Louis Brandeis published their seminal article, "The Right to Privacy," in 1890, they specifically identified the rollout of "[i]nstantaneous photographs" and "numerous mechanical devices" that threatened to ensure that "what is whispered in the closet shall be proclaimed from the house-tops."[1] Their response to these new risks was to establish the theoretical foundation for a body of law that could protect the individual right to privacy against such intrusions. And state courts and legislatures responded quickly by establishing a range of privacy rights at common law and in statute. More than half a century later, these common law rights were organized and systematized in a now famous article by William Prosser aptly named "Privacy."[2] The four privacy torts Prosser set out in that article have not provided a complete solution to the harms of invasive surveillance and abuse,[3] but they established a foundation upon which future policy could build.

The law has continued to evolve over the last 150 years as new technologies emerged and as new social, government, and business structures have changed the scale and impact of surveillance practices. The Supreme Court in the *Olmstead* case in 1928 infamously rejected a constitutional privacy challenge to warrantless wiretapping of private telephone calls, over the resounding dissent of Justice Brandeis, who emphasized that "[t]ime works changes, brings into existence new conditions and purposes. Therefore, a principle, to be vital, must be capable of wider application than the mischief which gave it birth."[4] The Court ultimately saw the wisdom in his words and the folly of that decision four decades later when they ruled in the *Katz* case that the Fourth Amendment protects against invasions of a reasonable expectation of privacy.[5]

[1] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[2] William L. Prosser, *Privacy*, 48 Cal. Law. Rev. 383 (1960).
[3] *See, e.g.*, Daniel J. Solove & Neil Richards, *Prosser's Mixed Legacy*, 98 Cal. L. Rev. 1887 (2010).
[4] *Olmstead v. United States*, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting).
[5] *Katz v. United States*, 389 U.S. 347, 388 (1967) (Harlan, J., concurring).

Congress the next year passed the Wiretap Act of 1968, creating the robust oversight scheme we now know today and also criminalizing the intentional interception of private communications.[6]

We have witnessed a profound technological and cultural shift towards widescale surveillance in the fifty years since the Wiretap Act was passed. In 2002, EPIC launched a campaign called "Observing Surveillance" to document the widespread use of surveillance cameras in our nation's capital,[7] and that trend has increased exponentially with the marketing of direct-to-consumer and direct-to-business camera products, including those integrated into smartphones, doorbells, security lights, sunglasses, and other connected devices. These products and advances in digital camera technology have made it near impossible to "observe surveillance," as it is possible for anyone to capture high-quality photographs and videos. In 2007, the first generation of the iPhone featured a 2 megapixel camera, roughly equivalent to HD video; [8] some smartphones available today feature 48 megapixel cameras, far beyond 4K-quality images[9]—to put it another way, this is the difference between printing a clear image on a 5x7 index card and printing an equally clear image on a two foot poster.[10] These advanced capabilities allow for detailed photographs to be captured at a distance,[11] and there have been even more dramatic advancements in localized security cameras and in more widescale aerial surveillance systems, which can be integrated with Facial Recognition and other AI-based analytics and tracking capabilities.

---

[6] 18 U.S.C. § 2511.
[7] EPIC, *Observing Surveillance* (2002), https://observingsurveillance.org.
[8] James Bareham, *The iPhone 7 Plus vs. the original iPhone: a camera showdown*, The Verge (Sep. 14, 2016) https://www.theverge.com/tldr/2016/9/14/12917512/original-iphone-camera-vs-iphone-7-photo-comparison.
[9] Press Release, *Apple debuts iPhone 16e: A powerful new member of the iPhone 16 family*, Apple Newsroom (Feb. 19, 2025), https://www.apple.com/newsroom/2025/02/apple-debuts-iphone-16e-a-powerful-new-member-of-the-iphone-16-family/.
[10] Stephen Shankland, *The iPhone 14 Pro Cameras Are a Big Leap for Photo Enthusiasts*, CNET (Sep. 26, 2022), https://www.cnet.com/tech/mobile/iphone-14-pro-cameras-are-a-big-leap-for-photo-enthusiasts/.
[11] This capacity is not limited strictly to "cameras" as we think of them, because thanks to the continuing miniaturization of hardware there are now lens-less image sensors, thinner than one millimeter, that are capable of digitally interpreting light to produce images with resolution roughly equivalent to a high-density emoji. *See, e.g.,* Sunetra K. Mendis & Sabrina E. Kemeny, *A 128 x 128 CMOS Active Pixel Image Sensor for Highly Integrated Imaging Systems*, IEEE, Int'l Electron Devices Meeting, JPL Open Repository 93-1773 (1993) https://ntrs.nasa.gov/citations/20060039496 (128x128 pixels); Vivek Boominathan et al., *Recent Advances in Lensless Imaging*, 9 Optica 1 (Dec. 22, 2021), https://pmc.ncbi.nlm.nih.gov/articles/PMC9634619/.

Recording devices have also become much smaller and more precise. Microphones and other audio sensing devices can capture the contents of our speech with increasing audio quality. And developments in artificial intelligence make it easy for nearly anyone to process that audio, including to clone an individual's voice or make inferences about the speaker's physiological state, which can be done using fewer than two seconds of voice recording data.[12] And sensitive information about us, including our movements, social activities, beliefs, and health status can increasingly be inferred from data generated by cell phones and embedded sensors around us that pinpoint our location.

The rapid expansion of cloud storage capacity has made it trivial to store thousands of hours of video and audio data.[13] So where in the past a CCTV surveillance camera might have captured a relatively low resolution image and stored it for a few days until the system deleted it to make room for new recordings, now high resolution images (including night vision and other advanced capabilities) can be automatically uploaded, stored, and analyzed in the cloud over months and years.

There has also been a notable shift in market and culture toward what Professor Chris Gilliard and David Golumbia refer to as "luxury surveillance," or "surveillance that people pay for and whose tracking, monitoring, and quantification features are understood by the user as

[12] *See*, Hannes Diemerling et al., *Implementing Machine Learning Techniques for Continuous Emotion Prediction from Uniformly Segmented Voice Recordings*, 15 Front Psych. 1300996 (Mar. 20, 2024), https://pmc.ncbi.nlm.nih.gov/articles/PMC10987695/; Subramanian Suganya & Eugene Y.A. Charles, *Speech Emotion Recognition Using Deep Learning on Audio Recordings*, IEEE (2019), https://ieeexplore.ieee.org/document/9023737; *but see* Abigail Kunkler et al., Comments to Autoriteit Persoonsgegevens (Dutch DPA) on AI Systems for Emotion Recognition in the Areas of Workplace or Education Institutions: Prohibition in EU Regulation 2024/1689 (AI Act), EPIC (Dec. 17, 2024), https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/.

[13] Orin S. Kerr, *The Next Generation Communications Privacy Act,* 162 Univ. Penn. L. Rev. 373, 391 (2014), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1546&context=penn_law_review ("Computer storage costs have dropped by a factor of ten roughly every four years for the last thirty years. The cost of storing a single gigabyte of data has dropped from about $85,000 in 1984 to about five cents in 2011.") (internal citations omitted); *see also,* Eldar Haber, *The Wiretapping of Things*, 53 U. Cal. Davis L. Rev. 733, 776 (2019) (citing to William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1207-09 (2010) and to Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. Telecomm. & High Tech. L. 359, 386–87 (2010)).

benefits they are likely to celebrate."[14] Connected devices in the home, office, and in other shared spaces have proliferated, and many now come equipped with microphones, cameras, and other sensors. These devices can enable features that their owners want, but to a guest or bystander in a shared or semi-private space they could incidentally become surveillance devices capturing private communications and interactions.[15]

There has also been a significant increase in video recording by individuals using smartphones, which are now owned by the vast majority of American adults, or by other handheld (or worn) camera-enabled devices. These recordings, even if made intentionally and not surreptitiously, can cause harm to bystanders and other unwilling participants as well. Constant recording combined with the compulsive influences of social media can pose especially significant risks to children, who can become the unwitting subjects of surveillance.[16] Research has also shown that the presence of cell phone cameras in schools, enabling easy recording and rapid spread via social media, has played a role in precipitating and exacerbating violent fights between students.[17]

These developments have led to a significant loss of practical control over when and how images, recordings, and other information about our conversations and actions are being collected. And these capabilities have been used to malicious and abusive ends. It is unfortunately not surprising that those who seek to control, manipulate, and abuse others are ready and willing to use these technologies against their victims. For example, landlords have

[14] Chris Gilliard & David Golumbia, *Luxury Surveillance*, Real Life (July 6, 2021), https://reallifemag.com/luxury-surveillance/.
[15] *See, e.g.,* Eimann Saqib et al., *Bystander Privacy in Smart Homes: A Systematic Review of Concerns and Solutions*, ACM Transactions on Computer-Human Interaction (forthcoming, paper accepted on Mar. 14, 2025), https://dl.acm.org/doi/abs/10.1145/3731755.
[16] *See, e.g.,* Libby Morehouse, *The Kids Are Not Alright: A Look into the Absence of Laws Protecting Children in Social Media*, 44 Loyola of Los Angeles Ent. L. Rev. 74 (2024), https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1663&context=elr.
[17] *See* Natasha Singer, *How Student Phones and Social Media Are Fueling Fights in Schools*, N.Y. Times (Dec. 15, 2024), https://www.nytimes.com/2024/12/15/technology/school-fight-videos-student-phones.html.

misused smart locks to surveil, track, or intimidate their tenants.[18] These invasions, especially where they involve the non-consensual collection and use of images of our bodies and recordings of our interactions with families and loved ones, strike at the "moral and legal right" that Professor Danielle Citron so aptly coined as "Intimate Privacy."[19] Yet so far we are failing to take adequate steps to protect this essential right, and all too often people are abused by perpetrators that leverage these recording technologies.[20] Indeed, when smart devices are built into the environment, for example a hotel room, it leaves us all vulnerable to such abuse.[21]

2. Connected devices and embedded sensors pose significant threats to bystander privacy, but transparency standards and design interventions can mitigate some of the harms.

In a mostly analog world, an individual maintains significant control over what information they reveal to others in semi-public and shared spaces—they can choose whom to speak with, what to say, and whether to show or share more with others. But as the world around us has become more digitized and connected, any sense of individual control slips away. We don't have a meaningful choice not to go to the pharmacy if they install a new advanced camera system equipped with facial recognition. We are not going to refuse to visit our friends or to walk down the street because the houses now have doorbell cameras with high-definition recordings. And we won't cancel our vacation because the hotel or condo where we are staying has a voice-activated speaker system that might inadvertently capture our intimate conversations. Life in the

[18] Kim Lyons, *Amazon Alexa for Residential will let the voice assistant power apartment complexes*, The Verge (Sep. 3, 2020), https://www.theverge.com/2020/9/3/21419812/amazon-alexa-residential-apartment-privacy.
[19] Danielle Citron, *The Fight for Privacy* 106 (2022).
[20] One survey of several thousand people from Australia, New Zealand and the UK found that one in three respondents reported that nude or sexually explicit images had been captured of them without their consent; the actual percentage is likely higher as most people do not learn that such images of them have been captured and shared. Real-world examples include an electrician installing a camera in the women's changing room at a police station. In Louisiana, a man duct-taped a miniature camera to the inside of a urinal in the men's bathroom of his workplace. Danielle Keats Citron, *The Fight for Privacy* 29 (2022); *Id.* at 31 (recounting how a New York hotel employee placed a hidden camera in the bathroom of a guest room and posted recordings of the guest taking off their clothes to several porn sites under the guest's real name, then sent the guest threatening emails referencing the guest's school and employer, demanding the guest send him nude images and videos or else he would distribute the recordings further).
[21] Citron, *The Fight for Privacy* 7 (2022); *id.* at 29 (noting that hotel rooms and doctors' offices are prime targets for surreptitious collection of non-consensual intimate images).

era of "always on" (and always recording) devices imposes significantly on our privacy, and in return we must collectively call on industry and government leaders alike to mitigate these harms by adopting more privacy protective standards and practices.

Twenty years ago, Professors Jerry Kang and Dana Cuff published a critical paper that considered (and predicted) the impacts of wide scale digitization and connectivity, which they referred to as "pervasive computing."[22] They explained how the same trends that were then apparent about unrestrained data collection in the online ecosystem would likely carry over into our physical spaces as well with the rollout of connected devices and censors, with a major difference being that we have no way "log out" of the world around us.[23] They used the hypothetical example of a mall in this future era to identify the risks and issues posed by pervasive computing, and proposed a set of design principles and legal standards in response to advance the values of Privacy, Transparency, Open Access, and Publicity.[24] First among them was a baseline privacy protection to limit collection and use of information by a connected device to what is functionally necessary based on that devices use or purpose.[25] And next was a transparency right to ensure that people not only know the basis of any decisions to limit or deny their access to the hypothetical mall, but also to design the connected devices in such a way that they give patrons the ability to know what devices are there, what they are collecting, and when they are active.[26] We see echoes of this in recent product designs that turn lights on when a device camera or microphone is active.[27] These proposals resonate even more now that so much of what they predicted has come to pass. Indeed, we have already seen the problems that can

[22] *See, e.g.,* Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 65, Wash. And Lee L. Rev. 93, 106 (2005) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=626961 (quoting Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 Stan.. L. Rev. 1193, 1198-99 (1998)).
[23] *Id.* at 107.
[24] *Id.* at 134–45.
[25] *Id.* at 134–35.
[26] *Id.* at 136–38.
[27] *See, e.g.,* The Walt Disney Co., *Frequently Asked Questions About "Hey Disney!"* (2025) ("You'll know the device is listening to your request when the blue bar lights up."), https://privacy.thewaltdisneycompany.com/en/resort-hey-disney/.

arise from deployment of access controls[28] based on facial recognition cameras, both when they work as intended[29] and when they malfunction.[30]

These technological developments frustrate consumers' expectations of privacy in public, semi-private, and traditionally private spaces. In the last ten years, there have been numerous examples of consumers being horrified to learn of the different ways data about them had been surreptitiously collected by their devices, be they Smart TVs[31] or cars.[32] While the average American may have thought nothing of being seen walking to their local pharmacy on any given day, that feeling is likely to be very different when every such trip, and indeed any trip anywhere, is captured, stored indefinitely, and analyzed to make automated decisions about that person—from marketing offers to product pricing to social scoring based on where they go and how often; such profiles have been in development in the digital sphere pulling data from multiple sources for many years.[33] Even setting aside the predictably mass scale at which such systems tend to operate, there are also serious risks to Americans' privacy and personal safety even when the technology is only being used by a single individual. It is not hard to imagine how an

[28] *See, e.g.,* Kang & Cuff, *Pervasive Computing: Embedding the Public Sphere*, *supra* note 22.
[29] Mia Sato, *Madison Square Garden's Surveillance System Banned This Fan Over His T-shirt Design*, The Verge (Mar. 28, 2025), https://www.theverge.com/news/637228/madison-square-garden-james-dolan-facial-recognition-fan-ban; Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N. Y. Times (Dec. 23, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.
[30] Varsha Bansal, *How I Investigated the Impact of Facial Recognition on Uber Drivers in India*, Pulitzer Center (Aug. 10, 2023), https://pulitzercenter.org/how-i-investigated-impact-facial-recognition-uber-drivers-india.
[31] Press Release, *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent*, Fed. Trade Comm'n. (Feb. 6, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million.
[32] Press Release, *FTC Takes Action Against General Motors for Sharing Drivers; Precise Location and Driving Behavior Data Without Consent*, Fed. Trade Comm'n. (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data.
[33] *See, e.g.,* Staff Report, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, Fed. Trade Comm'n., Appendix B (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

unscrupulous property owner—be they a landlord[34] or homeowner association (HOA)[35] or a condo rental host[36] or a taxi driver or just a nosy neighbor—or alternatively how an outright abusive partner, might leverage cheap, portable,[37] tiny, connected devices to surreptitiously target and surveil their victims or unfortunate bystanders.

Facilitating awareness of these capabilities among consumers is an important step but can only be a partial solution to these problems, as victims and bystanders are unlikely to be the ones purchasing the devices capable of this surveillance. While thoughtful product design—such as a hardwired indicator light for when a camera or microphone is active[38] or push notifications alerting a user that a tracking device is following them[39]—can address some of these problems, we must continue to anticipate how malicious users, or third parties might circumvent these protections and improve upon product design accordingly.

There have been significant efforts in recent years to require more clear and comprehensible information about whether products contain cameras and microphones (and what

---

[34] Ángel Díaz, *When Police Surveillance Meets the 'Internet of Things',* Brennan Ctr. For Just. (Dec. 16, 2020) https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things (citing to Giniia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?,* N.Y. Times (Mar. 31, 2019), https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html and Alfred Ng, *Your Landlord Turns Your Apartment Into a Smart Home. Now What?,* CNET (Mar. 7, 2019), https://www.cnet.com/home/smart-home/your-landlord-turns-your-apartment-into-a-smart-home-now-what/).

[35] Díaz, *When Police Surveillance Meets the 'Internet of Things'* (2020), *supra* note 34 (citing to Ella Fassler, *Neighborhood Watch Has a New Tool: License-Plate Readers*, Medium (Nov. 12, 2020), https://onezero.medium.com/neighborhood-watch-has-a-new-tool-privately-owned-license-plate-readers-302f296abb27).

[36] Tyler Lacoma, *7 Ways to Spot Hidden Cameras in Your Airbnb Rental,* CNET (Apr. 8, 2025) https://www.cnet.com/home/security/spot-hidden-cameras-in-your-airbnb-rental/.

[37] *See* Haber, *The Wiretapping of Things supra* note 13 at 779 (noting that bugs are generally not portable, but many IoT devices are portable or even wearable).

[38] Such an indicator light could likely easily be covered by a malicious user. Moreover, where consumers are aware that there is a camera on an IoT device, they can cover the lens, but it is often impossible for consumers to similarly disable a microphone. *See, e.g.,* Bryson R. Payne et al., *Siri Gets a Subpoena: Unintended Social, Ethical and Legal Consequences of the Internet of Things*, Nat'l Cyber Summit 13, 2, 4 (2017) https://louis.uah.edu/cyber-summit/ncs2017/ncs2017papers/13/. This is especially problematic when it is known that intelligence agencies have used devices like Smart TVs to surreptitiously record conversations after those devices appeared to have turned off. *See, e.g., id*. at 2 (citing to Liedtke, M., Anderson, M., Krishner, T. 2017. *WikiLeaks:CIA has targeted everyday gadgets for snooping*. Atlanta Journal-Constitution (March 7, 2017), http://www.myajc.com/news/2hJf1W4bl6bXwqbOiEIOGP/).

[39] For example, an abuser who is significantly more tech-savvy than their intended victim could bypass this by indicating that the device is registered to their victim or otherwise permanently silencing the notification the first time it appears.

data they collect). The Federal Communications Commission initiated a process through its U.S. Cyber Trust Mark program that could provide a mechanism for informing consumers about the surveillance capabilities of Internet of Things (IoT) devices. In a similar vein, there have been bipartisan bills introduced to address this issue, including the Informing Consumers about Smart Devices Act, [40] with a companion bill sponsored in the Senate,[41] which would require disclosing to the consumer prior to purchase that an IoT device contains a camera or microphone. While EPIC supports this type of measure generally, we encourage Congress to consider how it can provide more robust privacy protection against the surreptitious collection of Americans' geolocation information, their physiological state, or proxies for any of those data-points (for example using the strengths of wireless signals and names of nearby wireless networks to approximate location, rather than using GPS).[42]

Again, however, EPIC emphasizes that consumer awareness is only a partial solution. There are well-documented instances of IoT device security being subverted by malicious third parties, resulting in strangers taking over baby monitors[43] or doorbell cameras.[44] Unfortunately,

---

[40] Informing Consumers about Smart Devices Act, H.R. 859, 119th Cong. (1st Sess. 2025) https://www.congress.gov/bill/119th-congress/house-bill/859.
[41] Informing Consumers about Smart Devices Act, S. 28, 119th Cong. (1st Sess. 2025), https://www.congress.gov/bill/119th-congress/senate-bill/28.
[42] *See, e.g.,* U.S. Patent No. 9,591,457 B1 (May 24, 2015) (issued Mar. 7, 2017), https://patents.google.com/patent/US9591457B1/en; John Kruman & Eric Horvitz, *LOCADIO: Inferring Motion and Location from Wi-Fi Signal Strengths*, Mobiquitous 2004 (First Annual International Conference on Mobile and Ubiquitous Systems (Aug. 22 2004), https://erichorvitz.com/locadio.pdf ; Atul Gosai & Rushi Raval, *Real Time Location Based Tracking Using WIFI Signals*, 101 Int'l. J. of Comp. Sci. 21 (2014), https://www.ijcaonline.org/archives/volume101/number5/17684-8542/ ; Leon Wu & Ying Zhu, *Inferring Locations of Mobile Devices from Wi-Fi Data*, 7 Intelligent Inf. Mgmt. (Mar. 2015), https://www.scirp.org/journal/paperinformation?paperid=54423.
[43] Lily Hay Newman, *Millions of Web Camera and Baby Monitor Feeds Are Exposed*, Wired (Aug. 17, 2021) https://www.wired.com/story/kalay-iot-bug-video-feeds/ ; Press Release, *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.*, Fed. Trade Comm'n. (Feb. 7, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc ; *US parents warned on hacked baby webcams*, BBC (Jan. 28, 2016), https://www.bbc.com/news/technology-35427586.
[44] Lorenzo Franceschi-Bicchierai, *Popular video doorbells can be easily hijacked, researchers find*, TechCrunch (Feb. 29, 2024), https://techcrunch.com/2024/02/29/popular-video-doorbells-eken-tuck-hijacked-researchers/; Monika Grigutyè, *Ring hacked: Doorbell and camera security issues*, Nord VPN (Feb. 12, 2024), https://nordvpn.com/blog/ring-doorbell-hack/ ; Press Release, *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras*, Fed. Trade Comm'n. (May 31, 2023),

there are also well-documented instances of IoT devices being deliberately utilized by stalkers and abusers.[45] Our common understandings of privacy are also challenged by the persistent surveillance of passers-by captured by IoT devices, such as wearable cameras.[46] There is also always the danger of a product malfunction,[47] or of a company changing its policies without adequately informing the consumer,[48] especially in a way that frustrates the purchase decision the consumer made (i.e. the consumer would have purchased a device from a different company had it known the company would change its privacy policy[49]).

The development of devices like Apple's AirTags is an illustrative example of how companies can better anticipate misuse of their products and services prior to offering them in the marketplace. AirTags are portable tracking devices about as large as a U.S. half dollar coin that were first released in 2021 to help users locate their keys, bag, jacket, etc.[50] By the end of

---

https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users (noting not only strangers but company employees illegally surveilled customers).

[45] *What is Stalkerware?*, Coalition Against Stalkerware, https://stopstalkerware.org/ (last accessed May. 19, 2025); Tamsin Rose & AAP, *Tracking devices increasingly used by DV offenders to 'stalk, harass, intimidate and monitor victims',* The Guardian (Jun. 24, 2024), https://www.theguardian.com/world/article/2024/jun/25/tracking-device-domestic-violence-offenders-stalking-apple-find-my-friends ; Kate Lyons, *Stalkers using bugging devices and spyware to monitor victims*, The Guardian (Feb. 13, 2018), https://www.theguardian.com/uk-news/2018/feb/13/stalkers-using-bugging-devices-and-spyware-to-monitor-victims.

[46] Zahra Takshid, *Wearable AI, Bystander Notice, and the Question of Privacy Frictions*, 104 Boston L. Rev. 1087, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4693396.

[47] Eugene Kim, *Amazon Echo secretly recorded a family's conversation and sent it to a random person on their contact list,* CNBC (May 24, 2018), https://www.cnbc.com/2018/05/24/amazon-echo-recorded-conversation-sent-to-random-person-report.html.

[48] *See, e.g.*, Wes Davis, *LinkedIn is training AI models on your data*, The Verge (Sep. 18, 2024), https://www.theverge.com/2024/9/18/24248471/linkedin-ai-training-user-accounts-data-opt-in ; Melissa Heikkilä, *How to opt out of Meta's AI training*, MIT Tech. Rev. (Jun. 14, 2024), https://www.technologyreview.com/2024/06/14/1093789/how-to-opt-out-of-meta-ai-training/ ; *How to stop your data from being used for AI training,* U.S. PIRG (Nov. 27, 2024), https://pirg.org/edfund/resources/how-to-stop-your-data-from-being-used-for-ai-training/ ; Makena Kelly & Nick Statt, *Amazon confirms it holds on to Alexa data even if you delete audio files*, The Verge (Jul. 3, 2019), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy.

[49] *See, e.g.,* Kim Lyons, *Amazon Alexa for Residential will let the voice assistant power apartment complexes*, The Verge (Sep. 3, 2020), https://www.theverge.com/2020/9/3/21419812/amazon-alexa-residential-apartment-privacy (noting that Amazon didn't always delete Alexa data even when users told it to, and employed humans to listen to and transcribe Alexa recordings); Scharon Harding, *Everything you say to your Echo will be sent to Amazon starting on March 28*, ArsTechnica (Mar. 14, 2025), https://arstechnica.com/gadgets/2025/03/everything-you-say-to-your-echo-will-be-sent-to-amazon-starting-on-march-28/.

[50] Press Release, *Apple introduces AirTag*, Apple Newsroom (Apr. 20, 2021), https://www.apple.com/newsroom/2021/04/apple-introduces-airtag/.

that same year, there was already reason to suspect these devices were being misused to surreptitiously track people.[51] By 2023, a class action complaint had been filed against Apple, alleging not only real-world harms that had occurred since the product's release but also alleging that the company had not heeded the warnings of advocates and technologists about the potential for these harms prior to the product's release.[52] By May 2024, Apple and Google had released industry specifications to allow for smartphone-based user alerts if a device was likely being used to track the smartphone user, even if that device was not within the company's own product ecosystem.[53] This is a very positive development, but it should not have taken actual harm and resulting litigation for the manufacturers of tiny, cheap, portable surveillance devices to overcome the friction in developing industry standards to enact safeguards to prevent malicious product misuse. Nor should federal regulators have had to step in to police the consumer privacy and security failings of doorbell cameras and baby monitors;[54] the companies themselves should have anticipated and guarded against these harms—especially as under the current Administration federal consumer protection agencies are being scaled back to the point of ineffectiveness.[55]

---

[51] Ryan Mac & Kashmir Hill, *Are Apple AirTags Being Used to Track People and Steal Cars?,* N. Y. Times (Dec. 30, 2021), https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html.

[52] First Amended Class Action Complaint, *Hughes et al., v. Apple, Inc*., Case No.: 3:22-cv-07668-VC , ¶ 10 (N.D. Cal. Oct. 6, 2023), https://cdn.arstechnica.net/wp-content/uploads/2023/10/Hughes-v-Apple-Amended-Complaint-10-12-2023.pdf.

[53] *Apple and Google deliver support for unwanted tracking alerts in iOS and Android,* Apple Newsroom (May 13, 2024), https://www.apple.com/newsroom/2024/05/apple-and-google-deliver-support-for-unwanted-tracking-alerts-in-ios-and-android/.

[54] *See, e.g.*, Press Release, *FTC Approves Final Order Settling Charges Against TRENDnet, Inc.*, Fed. Trade Comm'n. (Feb. 7, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc; Press Release, *FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras*, Fed. Trade Comm'n. (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users; *see also* Notice of Apparent Liability for Forfeiture, *In re: Eken Group Limited*, FCC-24-122 (Nov. 21, 2024), https://www.fcc.gov/document/fcc-proposes-fine-against-eken-submitting-untruthful-information; Fed. Commc'ns Comm'n, *Starks Letters to Amazon, Sears, Shein, Temu, and Walmart* (Mar. 8, 2024), https://www.fcc.gov/document/starks-letters-amazon-sears-shein-temu-and-walmart.

[55] *See, e.g.,* Kate Berry, *Trump's CFPB has dropped half of all pending litigation*, American Banker (May 14, 2025), https://www.americanbanker.com/news/trumps-cfpb-drops-more-than-half-of-all-pending-litigation ; Filip Timotija, *Trump administration to cut 90 percent of CFPB in latest layoffs: Reports*, The Hill (Apr. 17, 2025),

3. Privacy law has traditionally provided weaker protections for recording and monitoring in spaces that are not akin to the private sphere of the "home".

While modern privacy is rooted in the problem of private affairs spilling out into the broader public sphere, it is also built upon the historical roots of the inviolability of the home as a private sphere. Indeed, there is a long chain of cases and statutes "protecting the ability of individuals to enjoy undisputed tranquility in the home" as Professor Margot Kaminski puts it.[56] But in other shared spaces the right to limit monitoring and tracking has been more circumscribed. This is, in part, due to the interplay between privacy and speech rights, which make penalizing the dissemination of private information more restricted.[57]

Still many states have adopted eavesdropping statutes to limit surreptitious recording and voyeurism (so-called "Peeping Tom") statutes to limit capturing images or video of an individual in an area where they have an expectation of privacy. Federal and state wiretap acts typically only protect against third-party interception, but some states require that both parties to a communication consent before it can be recorded. And substantial progress has been made in the last decade to combat the scourge of Image-Based Sexual Abuse and other online related intimate privacy violations, thanks in large part to the work of Professors Danielle Citron and Mary Anne Franks and the Cyber Civil Rights Initiative.[58] Just this week, the TAKE IT DOWN Act is expected to be signed into law, criminalizing the nonconsensual distribution of intimate images, which is an essential step to take on these abusive practices and hold perpetrators accountable.[59]

---

https://thehill.com/business/5255231-trump-admin-to-cut-90-percent-of-cfpb-in-latest-layoffs-reports/ ; Jody Godoy, *Trump fires both Democratic commissioners at FTC*, Reuters (Mar. 19, 2025), https://www.reuters.com/world/us/trump-fires-both-democratic-commissioners-ftc-sources-say-2025-03-18/.

[56] Margot Kaminski, *Privacy and the Right to Record*, 97 B.U. L. Rev. 167, 207 (2017). *See, e.g.*, *Frisby v. Schultz*, 487 U.S. 747 (1988).

[57] *See* Neil Richards, *The Limits of Tort Privacy*, 9 J. Telecomm. & High Tech L. 357 (2011).

[58] *See* Cyber Civil Rights Initiative, *Legislative Reform* (2025), https://cybercivilrights.org/legislative-reform/.

[59] *See* Press Release, Cyber Civil Rights Initiative, CCRI Statement on the Passage of the TAKE IT DOWN Act (S. 146) (Apr. 28, 2025), https://cybercivilrights.org/ccri-statement-on-the-passage-of-the-take-it-down-act-s-146/.

When it comes to the broader scope of recording and monitoring in shared and semi-public spaces, there are several key statutory protections that are relevant, but fall short of establishing adequate protection given the scale of data collection that is now pervasive. The Stored Communications Act has been woefully outdated for decades,[60] and the Wiretap Act offers less protection than several states, allowing for one-party consent for recording the content of communications where some states require all parties to consent.[61] In the courts, privacy torts have developed through common law, but these are often ill-equipped to deal with the magnitude of privacy invasions capable from misuse of IoT data,[62] especially where some courts still fail to recognize non-monetary harms as sufficient to confer standing on plaintiffs,[63] which can preclude litigants from even being able to be heard.

In public spaces, individuals have a narrower reasonable expectation of privacy due to the possibility of being overheard. Merely overhearing or recording a conversation occurring in a public space that an individual is legally entitled to attend is not prohibited by the Wiretap Act or the intrusion tort. Under the federal Wiretap Act, individuals cannot be sued if they are parties to

[60] *See, e.g.* Orin S. Kerr*, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it,* 72 George Wash. L. Rev. 1208 (2004), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

[61] *See, e.g.,* Díaz, *When Police Surveillance Meets the 'Internet of Things'*, *supra* note 34; *Laws on Recording Conversations in All 50 States*, Matthiesen, Wickert & Lehrer, S.C. (Feb. 14, 2022), https://www.mwl-law.com/wp-content/uploads/2018/02/RECORDING-CONVERSATIONS-CHART.pdf.

[62] *See, e.g.*, Alexander H. Tran, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 Colum. J.L. & Soc. Probs. 263, 282 (2017) (noting the newsworthiness defense could swallow the rule for the tort of publication of private facts, citing to Harry Kalven, Jr., *Privacy in Tort Law: Were Warren and Brandeis Wrong?*, 31 Law & Contemp. Prob. 326 (1966)). The limitations of tort law are particularly apparent in the context of intimate images captured by hidden cameras, such as connected devices, for example due to the non-recoverable upfront costs of general tort suits, *see, e.g.*, Danielle K. Citron, *Cyber Civil Rights* , 89 Boston U. L. Rev. 61, 91 (2009), high evidentiary hurdles, *see, e.g.*, Ari Ezra Waldman, *A Breach of Trust: Fighting Nonconsensual Pornography*, 102 Iowa L. Rev. 709, 712 (2016), and other practical realities, *see, e.g.*, Danielle Keats Citron, *The Continued (In)visibility of Cyber Gender Abuse*, 133 Yale L. J. Forum 333, 358 (Nov. 22, 2023).

[63] *See, e.g.,* Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 101 B.U. L. Rev. 62 (2021), https://www.bu.edu/bulawreview/2021/07/21/standing-and-privacy-harms-a-critique-of-transunion-v-ramirez/ ; Eric N. Holmes, Cong. Rsch. Serv. LSB10629, *Privacy Law and Private Rights of Action: Standing After Transunion v. Ramirez* (2021), https://www.congress.gov/crs-product/LSB10629; Megan Iorio, *In Acheson Hotels v. Laufer, a Dangerous Opportunity for SCOTUS to Make it Harder to Establish Informational Standing*, EPIC (Oct. 4, 2023), https://epic.org/in-acheson-hotels-v-laufer-a-dangerous-opportunity-for-scotus-to-make-it-harder-to-establish-informational-standing/; *but see In Martizen v. ZoomInfo, Ninth Circuit Recognizes Privacy Plaintiff Has Standing to Sue,* EPIC (Sep. 21, 2023*),* https://epic.org/in-martinez-v-zoominfo-ninth-circuit-recognizes-privacy-plaintiff-has-standing-to-sue/.

the conversations they can overhear.[64] One party consent wiretap laws exempt those individuals from liability unless they are engaging in criminal or tortious activity.[65] Specifically, the recording of conversations for the purpose of a crime or other tortious activity must be a separate crime than the mere eavesdropping or intent to eavesdrop, such as blackmail using the recorded conversation.[66] This becomes an issue in states with two party consent laws, though. If all parties to a communication must consent to the recording, then walking in public with glasses equipped with a microphone could become an unintentional wiretap.

However, even if the interception of the communication is not a wiretap violation, the recording in a public space could still constitute an intrusion upon seclusion claim if the targeted individuals had a reasonable expectation of privacy, the recorder intentionally "penetrated some zone of physical or sensory privacy", and the intrusion was "highly offensive to a reasonable person." For example, a car crash on the interstate occurs in a public space.[67] A tv producer taking a video of the crash from the street and a tv producer making a nurse surreptitiously wear a wireless microphone that picks up her conversation are treated differently because of the difference in the level of intimacy, or zone of privacy, of the two different types of content collected.[68] There is a tangible difference between the recording a car crash from the side of the road a hundred feet away in a public space, compared to recording a conversation between a medical professional and a patient regardless of location. As this zone of privacy strengthens, so too does the claim of the recorded individuals. We know that when a landlord places a microphone in a rental property to record their tenant's conversations it is clearly an intrusion

[64] *Planned Parenthood Fed'n. of Am., Inc. et al. v. Newman et al*., 51 F.4th 1125, 1133 (9th Cir. 2022) (quoting *Cohen v. Cowles Media Co.,* 501 U.S. 663, 669(1991)), *cert. denied*, 144 S. Ct. 88 (2023)).
[65] 18 U.S.C. § 2511(2)(d).
[66] *Planned Parenthood Fed'n. of Am. et al*., 51 F.4th at 1135–36.
[67] *Shulman v. Group W Productions, Inc.,* 955 P.2d 469, 490 (Cal. 1998).
[68] *Id.* at 494.

upon seclusion.[69] And, similarly, placing a tap on an individual's phone line as a tactic in a months-long harassment campaign would also constitute an intrusion.[70]

The analysis become more complicated, though, when the entity intruding on an individual's zone of privacy is a company, rather than a natural person. An insidious but frustratingly common example of the recording of intimate conversations in private homes is done by smart home listening devices, such as Amazon's Alexa and Google Home. Both products have privacy policies disclaiming any liability and requesting consent to use their microphones—however, without adequate privacy laws containing data minimization standards, there is nothing stopping these companies from recording these conversations and collecting information about the individuals speaking. Individuals who buy the device and install them in a space may have consented to the device's terms and conditions and thereby consented to the collection of some of their communications by the device. But even in the case where a device's owner understands and consents to its use for recording, that does not resolve the rights of bystanders like a person who is visiting a friend who owns an Alexa, or an individual visiting the dentist who uses a Google Home as a music speaker. In those situations, neither individual has consented to the listening or recording of their conversations. Advocates are currently demanding accountability and transparency from these companies to stop this egregious erosion of privacy, litigating in both Washington state[71] and California.[72]

While both cases are ongoing with various issues of law and fact yet to be resolved, the courts seem to lean towards allowing the terms and conditions of these products to shield wiretap liability. In Washington state, a user of a smart home device is deemed to consent to the listening and recording of their conversations if they accept the terms and conditions of the device, which they consent to in the process of purchasing and setting up the device.[73] This consent, however,

[69] *Hamberger v. Eastman,* 206 A.2d 239 (N.H. 1964).
[70] *Nader v. Gen. Motors Corp. et al*. 255 N.E. 2d 765 (N.Y. 1970).
[71] *Garner v. Amazon.com, Inc*., 603 F.Supp.3d 985, 999 (W.D. Wash. 2022).
[72] *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 818 (N.D. Cal 2020).
[73] *Garner v. Amazon.com, Inc*., 603 F. Supp. 3d at 999.

is nominal at best. Notice and consent practices rarely end in consumers who know precisely how their data is collected, used, and deleted, much less understanding the ramifications of that data processing.[74]

Consumers should have access to information about when and how their voice or image is being recorded, such as through device registries, digital beacons, and other physical indicators when a device's microphone is actively listening. Even those who don't nominally consent to the listening and recording of conversations face legal challenges to redress. For those who don't accept the privacy policies of these devices, there is a conflict between state and federal wiretap law as to what rights apply. The court found that under Washington state's wiretap law, any person who doesn't affirmatively accept the terms and conditions of these products may have a colorable wiretap claim regardless of whether they used a trigger phrase such as "Hey Alexa" or not, whereas the court held that under the Federal wiretap law the use of a trigger phrase implied consent such that the interception, should it exist, would be exempted.

Further muddying the waters is the federal Wiretap Act's 'ordinary course of business' exemption. Devices, particularly telecommunications equipment, may generally intercept communications within the definition of the Wiretap Act. The Act exempts those devices that are expressly furnished to the user in the ordinary course of business and is used by the user or law enforcement in the ordinary course of business.[75] A major question posed by the smart home listening devices is whether or not its listening to and recording conversations to listen for trigger phrases such as "Hey Google" constitutes the ordinary course of business of the provision and use of the product. Neither party in the California case briefed the issue in depth, and the court refused to rule definitively; however, the judge explicitly stated in *dicta* that raising the ordinary course of business defense "does not preclude [] Wiretap Act claims." [76] We encourage Congress

[74] Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. Univ. L. Rev. 1461 (2019), https://scholarship.law.bu.edu/faculty_scholarship/3067.
[75] 18 U.S.C. § 2510(5)(a).
[76] *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d at 818.

to investigate the scope of abusive recording cases and consider whether Wiretap Act protections could be strengthened to prevent these harms.

The concern with these smart home listening devices isn't just that the companies are listening to these conversations, but also that the companies are recording and storing this data in ways that make it more likely to be leaked or breached. In 2023, the Federal Trade Commission and the Department of Justice penalized Amazon for recording and refusing to delete voice data of children under 13 through Alexa devices in violation of the Children's Online Privacy Protection Act.[77] Amazon harvested the data from these recordings and processed them to "improve its Alexa algorithm[,]" including personal information from children under the age of 13. This secondary processing itself is harmful, but it also exposes these databases to major cybersecurity risks and is query-able by a simple law enforcement subpoena. The information in those databases is highly sensitive, especially if it is stored in conjunction with the rest of Amazon's unprecedented trove of personal data, with no deletion policy.

4. This Subcommittee should investigate the extent to which privacy threats posed by widespread monitoring in semi-private and other shared spaces are exacerbated by cloud storage, data analytics, and viral dissemination systems.

The defense and preservation of privacy has always relied upon the intertwined efforts of lawmakers, technologists, advocates, and individuals. Technological advances have in many cases created new threats to privacy that require the establishment of new rules, norms, and standards. And we find ourselves now in a period where the rapid expansion of pervasive computing has embedded tracking capabilities in our lived environment. This is a time for action on all fronts to work to preserve the values enshrined in our Constitution and our laws, to ensure that we as individuals do not fall victim to the eradication of privacy by path of least resistance.

[77] Press Release, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests,* Fed. Trade Comn'n. (May 31, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

We appreciate the opportunity to draw public attention to these issues and to assist the Subcommittee in this inquiry. There is an opportunity here to identify standards and policies that can strengthen privacy protections and improve transparency about the devices and systems embedded in our physical environments. EPIC has focused in recent years on the need for a strong data minimization standard to protect individuals against the risks of overcollection and unauthorized uses of their data.[78] And we have seen some positive developments in privacy enhancing designs of connected devices including stricter security standards, physical controls of recording features (e.g. a "microphone off" switch), and clear indications of when a device is recording. But a focused investigation of how these devices are designed and deployed would be valuable in guiding future policy in this area.

There should also be special attention paid to the data collection and security practices of the companies that provide internet service to these connected devices (and thereby have access to data that monitors people's locations and activities),[79] and to closely review the cybersecurity practices of companies that manufacture and operate connected devices. This could include an inquiry into whether there has been unauthorized access to the data collected by these devices and what measures that company has taken to prevent similar instances of unauthorized access in the future.[80] We encourage the committee to specifically prioritize devices or applications that could pose heightened risks to targets of stalkers or abusers, for example family tracking apps

[78] *See* EPIC, Data Minimization, https://epic.org/issues/consumer-privacy/data-minimization/.
[79] *See, e.g., FCC Fines Major U.S. Wireless Carriers for Selling Customer Location Data*, KrebsonSecurity (Apr. 29, 2024), https://krebsonsecurity.com/2024/04/fcc-fines-major-u-s-wireless-carriers-for-selling-customer-location-data/; *A Look At What ISPs Know About You, supra* note 3333 at iii-iv, 17, 22, 33, 36.
[80] *See, e.g., Industry Letter Re: Cyber Fraud Alert*, N.Y. State Dep't of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (alerting auto insurance industry to data breach threat actor pattern); *Comments of EPIC in re: the FTC's Proposed Order & Settlement with Marriott and Starwood* at 3-4 (Nov. 12, 2024), https://epic.org/documents/comments-of-epic-in-re-the-federal-trade-commissions-proposed-order-settlement-with-marriott-and-starwood/ (noting failure to correct known cybersecurity vulnerabilities).

provided by the largest telecommunications companies[81] or tracking or recording features offered via connected car services.[82]

* * *

This hearing raises important questions about the risks to privacy posed by advanced recording and monitoring technologies. These issues have become increasingly salient as these sensors become harder to detect and as monitoring capabilities are being embedded in our physical surroundings and even in private spaces. We look forward to the opportunity to continue to draw public attention to these emerging risks and work to develop stronger privacy protections and standards to protect individuals against abuse.

Thank you again for the opportunity to testify today.

[81] *See, e.g.*, Reply Comments of EPIC, et al., *In re: Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program, Supporting Survivors of Domestic and Sexual Violence*, WC Dkt. Nos. 11-42, 21-250, 22-238 at 5-8 (May 12, 2023), 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.
[82] *See, e.g.*, *EPIC Encourages FCC to Continue Advancing Five Principles to Protect Domestic Violence Survivors in Connected Cars Rulemaking* (May 29, 2024), https://epic.org/epic-encourages-fcc-to-continue-advancing-five-principles-to-protect-domestic-violence-survivors-in-connected-cars-rulemaking/.