LEGISLATIVE OFFICE BUILDING
1020 "N" STREET, SUITE 162
SACRAMENTO, CA 95814
(916) 319-2200

CHIEF CONSULTANT
JOSH TOSNEY

PRINCIPAL CONSULTANT
JULIE SALLEY

COMMITTEE SECRETARY
MIMI HOLTKAMP

Assembly
California Legislature

ASSEMBLY COMMITTEE ON
PRIVACY AND CONSUMER PROTECTION
REBECCA BAUER-KAHAN, CHAIR
ASSEMBLYMEMBER, SIXTEENTH DISTRICT

INFORMATIONAL HEARING
ASSEMBLY PRIVACY AND CONSUMER PROTECTION COMMITTEE

SOMEBODY'S WATCHING YOU: CALIFORNIANS' PRIVACY IN THE AGE OF MASS SURVEILLANCE

Tuesday, March 3, 2026
1:30 p.m.
State Capitol Room 437

BACKGROUND PAPER

I. INTRODUCTION

Data and personal information are the new extractive commodities of the age. Often compared to oil, data may be a more renewable resource, albeit at a cost to privacy, autonomy, democratic accountability, consumer choice, and indeed, the environment (in the form of massive energy costs for data centers, e-waste, and the mining of rare minerals).[1] The experts gathered for today's hearing will discuss the many ways Californians have lost the ability to live their lives in private and the implications of that loss. The hearing will begin with an examination of how and why California became the first state to include the right to privacy in its constitution and what has happened to that right in the intervening 50 years. The first panel will then discuss the tools businesses use to surveil consumers and workers to enhance their profits and the implications for Californians. The second panel will move from the focus on surveillance for profit to discussing the ways that local, state, and federal governments are using data collected by private businesses and conducting their own surveillance on the everyday activities of people residing in and visiting this state.

II. CALIFORNIANS' RIGHT TO PRIVACY

As Tracy Rosenberg of Oakland Privacy has detailed:

> In 1972, in the wake of revelations about the abuses of J. Edgar Hoover's FBI and the Cointelpro program, Californians, by a 62.9% yes vote, added the right to privacy to California's state constitution via Prop 11. ACA 51, introduced by assembly member Ken

[1] https://irisnrc.wisc.edu/wp-content/uploads/sites/1577/2021/06/Privacy-under-Surveillance-Capitalism.pdf.

Cory added privacy to the list of the inalienable rights of the people of the state and replaced the word "men" with the word "people" in the state constitution.

Cory battled opposition from private industry, the Department of Motor Vehicles and law enforcement, but was eventually able to corral support from 2/3 of both houses of the Legislature. Prop 11 went on the November 1972 ballot with an argument in support from State Senate Majority Leader George Moscone:

> *"The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American citizens. Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian."*
>
> *"The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives"*[2,3]

While elected officials and voters in the 1970s may not have fully appreciated technology's impacts on individuals' ability to live private lives, Assemblymember Cory and his fellow legislators did understand that the danger lay with technological advancements and the ease with which that technology would be "capable of monitoring, centralizing, and evaluating . . . information and making credible the fear of a womb-to-tomb dossier on each of us."[4]

Presently, California voters face an even greater "dictatorship of dossiers"[5] than their predecessors, with not only global governments' ability to monitor individuals' private lives, but also the near ubiquitous access to these dossiers afforded to private businesses and individuals willing to pay for them. There are more than 4,000 data brokers with dossiers on 98% of the people in the United States.[6] The largest data broker, Acxiom, has more than 10,000 data attributes on over 2.5 billion people in more than 60 countries.[7] The amount of data being

---

[2] Tracy Rosenberg, *Oakland Privacy*, April 26, 2025, co-sponsor letter for AB 1337 (Ward).
[3] Asm. Kenneth Cory Author Letter to the Legislative File. https://www.aclunorcal.org/campaigns-initiatives/california-constitutional-right-privacy/
[4] Asm. Kenneth Cory Author Letter to the Legislative File. https://www.aclunorcal.org/campaigns-initiatives/california-constitutional-right-privacy/
[5] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[6] Solove, Daniel J. *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, George Washington University Law School (Jan. 19, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103271.
[7] *Ibid.*

collected on people has increased dramatically over the last decade as businesses have figured out how to monetize this natural resource.[8]

III. SURVEILLANCE CAPITALISM

> *"It is possible to have surveillance capitalism, and it is possible to have a democracy. It is not possible to have both."* – Shoshana Zuboff

Picture this: Bird chirps emanating from your smart phone rouse you from your sleep. You're groggy, so you immediately check the application on your phone that collects the data from your Oura ring[9] to evaluate your sleep quality. If you have not slept well, you can anticipate advertisements any time you're online for melatonin and relaxation apps, which for $9.99 a month will help you improve the quality of your sleep. You listen to the news from your smart speaker, Alexa, and begin your day. While brushing your teeth, your Wi-Fi connected toothbrush measures and records how well and how long you brush. You pack your lunch: an apple and a pre-made salad that you ordered through a weekly meal delivery app. The WiFi-enabled refrigerator thoughtfully tells you that you are taking the last apple and asks if you want to add apples to the grocery list on your phone and if you would like to add "grocery shop" to your calendar.

Walking outside, your neighbor's security camera dutifully records the time you leave, what you're wearing, and who you are. Getting into your car, your regular podcasts immediately start playing and the maps application on your phone anticipates your route to your workplace parking garage telling you approximately how much time it will take to get there. As you drive, your car captures your location, the route you are taking, the speed with which you drive, and whether you are driving safely. Pulling into the parking garage, the automated license plate reader (ALPR) reads your plate and allows you entrance. As you park, your car obligingly notes where it is and the time that it arrived. Walking to your office, you grab coffee – your Apple Watch lights up to pay, and in your pocket, you feel the buzz of your banking app notification: $9.75 debited for a cappuccino and a muffin. (You're a conscientious tipper.) Next stop is work and the day commences in earnest.

By 9am, you have only used your smartphone to turn off your alarm and check your sleep quality. Yet by interacting with smart devices a half dozen times; you've generated several hundred data points of time stamps, transaction details, geo-tagged locations, and preferences.

These data points will likely be copied millions of times by various algorithms designed to send advertisements and then added to huge databases that enable marketers to create differing scenarios and outcomes to predict your behavior and your interests. Staggeringly, 2.5 quintillion bytes of data are generated every day (that's 18 zeros). That number will continue to grow. Search engines alone log around 6.4 billion searches per day.[10]

---

[8] *Ibid.*

[9] Oura ring is a wearable device that, according to its website, "[Collects] deeply personal health metrics and insights" and accurately reads "over 20 biometrics that directly impact how you feel." https://ouraring.com/

[10] Ebsworth, Jonathan, et al. *Surveillance capitalism: the hidden costs of the digital revolution* (2021).

Americans leave a trail of personal data with almost every action they take either in the physical world or online, including every website visited, credit card payment, and browser search.[11] This commodification of personal information has been dubbed "surveillance capitalism" by social psychologist Shoshana Zuboff. Essentially, surveillance capitalism is an economic system built on the secret extraction and manipulation of human data.[12] In an opinion piece for *The New York Times*, in 2021, Dr. Zuboff warned:

> As we move into the third decade of the 21st century, surveillance capitalism is the dominant economic institution of our time. In the absence of countervailing law, this system successfully mediates nearly every aspect of human engagement with digital information. The promise of the surveillance dividend now draws surveillance economics into the "normal" economy, from insurance, retail, banking and finance to agriculture, automobiles, education, health care and more. . . .
>
> An economic order founded on the secret massive-scale extraction of human data assumes the destruction of privacy as a nonnegotiable condition of its business operations. With privacy out of the way, ill-gotten human data are concentrated within private corporations, where they are claimed as corporate assets to be deployed at will.[13]

For almost two decades, experts have been warning about the erosion of our private lives. They note that this erosion is happening one small bit at a time, likely without people even noticing. With the advent of the internet and advances in technology, it is no longer easy for people to decide which aspects of their lives should be publicly disclosed. As Alex Preston noted the "Death of Privacy" in *The Guardian* a decade ago:

> We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and secret. . . . Insidiously, through small concessions that only mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web. . . the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.[14]

With the rapid growth in the development of Artificial Intelligence (AI) systems, particularly large-language models, personal information has become even more valuable as developers require ever-increasing amounts of data to train their foundation models. Going forward, AI

---

[11] Emile Ayoub and Elizabeth Goitein. *Closing the Data Broker Loophole*, The Brennan Center for Justice (Feb. 13, 2024).
[12] Zuboff, Shoshana, "You are the Object of a Secret Extraction Operation," *New York Times* (Nov. 12, 2021). https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html.
[13] *Ibid.*
[14] Preston, Alex. "The death of privacy." *The Guardian* (Aug. 3, 2014) https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston.

development will continue to increase developers' hunger for training data, fueling an even greater race for data acquisition than we have already seen in past decades.[15]

A 2023 investigation by Consumer Reports on the surveillance economy looked at the companies that share people's personal information with Facebook. Consumer Reports explains:

> One way to understand [the surveillance economy] is as the subset of consumer marketing in which the data being used is obtained from the surveillance, or covert observation, of ordinary consumer activities such as visiting websites, buying goods or services from an online or physical retailer, using one's credit card, and consuming entertainment content.
>
> The surveillance economy is "cross-contextual," meaning that it uses information about individuals that's been collected in one context—such as a website visit, an action taken in an app, or a visit to a physical location—and applies it to another context to affect how you are advertised to, what prices you see, and how you are otherwise treated.[16]

The study's findings reveal that 709 of their participants had their personal information shared by 186,892 companies. On average, each participant was represented in data shared by 2,230 different companies and some were represented in data shared by over 7,000 companies.[17]

California has a number of laws intended to protect our privacy. Among the most significant are the Information Practices Act, which creates restrictions on the state government's sharing of personal information; the Confidentiality of Medical Information Act, which restricts the sharing of personal health information; and the K-12 Pupil Online Personal Information Protection Act, which establishes privacy requirements for educational technology companies. Chief among the privacy laws is the California Consumer Privacy Act (CCPA)[18], which was amended by the voters through an initiative, the California Privacy Rights Act (CPRA), in 2020, that affords consumers the following rights when interacting with large businesses:

- The right to know the business or commercial purpose for collecting, selling, or sharing personal information; the categories of persons to whom the business discloses personal information; the specific pieces of information the business has collected; and the categories of third parties to whom the personal information was disclosed.
- The right to request deletion of personal information that a business has collected from the consumer, and the right to opt out of the sale of the consumer's personal information
- The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses.
- The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data.

---

[15] King, Jennifer and Meinhardt, Caroline. *Rethinking Privacy in the AI Era*. Human-Cantered Artificial Intelligence at Stanford University (Feb. 2024) https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.

[16] Don Marti, et al. "Who Shares Your Information with Facebook? Sampling the Surveillance Economy 2023," *Consumer Reports* (Jan. 2024) https://advocacy.consumerreports.org/research/report-who-shares-your-information-with-facebook/

[17] *Ibid.*

[18] AB 375; Chau, Ch. 55, Stats. 2018.

These laws primarily follow a consent model. In some cases, personal information cannot be shared without first seeking the consent of the individual. In the case of the CCPA, businesses may collect, use, share, and sell personal information as they see fit, unless the consumer opts out of the business sharing and selling their personal information. In a state that requires its residents to contact businesses and request that they delete their information or opt out of its collection in the first place, it would be virtually impossible for a California consumer to identify which companies have their personal information, much less request that it be deleted.[19] Despite these protections, a vast ecosystem of entities that harvest our personal information has emerged.

IV. SURVEILLANCE PRICING

Surveillance pricing, also known as individualized pricing, uses AI or other technology for the real-time processing of personal information about a consumer to set a price specific to them. The Federal Trade Commission (FTC) describes surveillance pricing as an ecosystem that uses "large-scale data collection to help sellers maximize their revenues by customizing the pricing, as well as the selection of products and services, offered to each consumer."[20]

It is important to distinguish surveillance pricing from dynamic pricing, which adjusts prices in response to market demand. For example, Ticketmaster uses dynamic pricing to increase ticket prices for all consumers when demand rises.[21] In contrast, surveillance pricing treats each consumer as their own economy, using algorithms to assess their willingness to pay based on personal information such as browsing history, purchase behavior, and location.

Examples of surveillance pricing. In 2012, *The Wall Street Journal* reported that the retailer Staples used an algorithm that set higher prices for consumers who lived further from a rival store.[22] Target also used an algorithm to adjust the price of a TV once a customer entered the parking lot, leading to a $5 million settlement with the City of San Diego for false advertising and unfair business practices related to surveillance pricing.[23] The *SF Gate* recently reported that

[19] In 2023, the Legislature passed the Delete Act, which required the California Privacy Protection Agency (CPPA) to develop a streamlined process that allows consumers to submit a request that every data broker that maintains any personal information delete the information related to that consumer held by the data broker. Once the Delete Act is fully implemented in August of this year, it will become significantly easier for consumers to request deletion from data brokers. Still, the onus remains on consumers to find California Privacy Protection Agency's website and request that their information be deleted.

[20] Federal Trade Commission, "Issue Spotlight: The Rise of Surveillance Pricing" (January 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[21] Cody Mello-Klein, "What is dynamic pricing and why is it hiking ticket prices for Oasis, Taylor Swift and your favorite artist?", *Northeastern Global News* (Oct. 2, 2024), https://news.northeastern.edu/2024/10/02/dynamic-pricing-ticketmaster-oasis-taylor-swift/.

[22] Jennifer Valentino-DeVries, Jeremy Singer-Vine and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal* (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

[23] Chris Hrapsky, "Target settles lawsuit alleging false advertising, overpricing; fined $5M", *KARE* (Apr. 27, 2022), https://www.kare11.com/article/news/local/kare11-extras/target-settles-ca-lawsuit-alleging-false-advertising-overpricing-fined-5m/89-ba4a5441-c38e-4c9f-b524-b0d13414042f.

Bay Area consumers are offered a higher price than users in either Phoenix or Kansas City for the same exact hotel reservations on various hotel booking websites.[24]

Moreover, the use of AI to set prices raises concerns regarding biases within the algorithms that may disadvantage different groups. A 2021 study from George Washington University found that Uber and Lyft charged, on average, higher prices for pickups and drop-offs in predominantly non-white neighborhoods or neighborhoods with lower incomes.[25] While it is unclear whether these disparities stem from market forces or algorithmic bias because of the opaque algorithms used by these companies to set prices, it is possible that algorithmic price-setting could reinforce structural inequities.

Federal Trade Commission investigation. Because businesses often operate without transparency, the extent of surveillance pricing remains uncertain. In the summer of 2024, the Federal Trade Commission (FTC) launched a study to investigate how companies leverage AI, other technologies, and consumer data to set individualized prices. A preliminary report released in January revealed that at least 250 businesses have adopted technologies capable of implementing surveillance pricing. Lina Khan, former FTC Chair, concludes in this report:

> Initial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage. The FTC should continue to investigate surveillance pricing practices because Americans deserve to know how their private data is being used to set the prices they pay and whether firms are charging different people different prices for the same good or service.[26]

V. TRACKING CALIFORNIANS' MOVEMENTS THROUGHOUT THEIR DAY

Tracking our location and movements. In the physical world, we cannot step out of our homes without being monitored and tracked. Cars collect location data everywhere we drive. Phones, our constant companions, collect location data everywhere we go. License plate readers and traffic cameras are at virtually every intersection, on freeways and toll roads, at the entrance of parking garages, and in store parking lots. These devices track the movement of every single car that passes by. Even if someone walks or rides a bicycle, security cameras on homes and business can capture their movements and their location. Our faces may not be captured by these cameras, but technological advancements can analyze a person's walk and movements using gait recognition technology and identify them.[27] In addition, most stores and businesses use security cameras and images from those cameras can easily be run through facial recognition systems to

---

[24] Keith A. Spencer, "Hotel booking sites show higher prices to travelers from Bay Area," *SFGATE* (Feb. 3, 2025), https://www.sfgate.com/travel/article/hotel-booking-sites-overcharge-bay-area-travelers-20025145.php.

[25] Akshat Pandey and Aylin Caliskan, "Disparate Impact of Artificial Intelligence Bias in Ridehailing Economy's Price Discrimination Algorithms" *arXiv* (May 3, 2021), https://arxiv.org/abs/2006.04599.

[26] Federal Trade Commission, "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices" (Mar. 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[27] *Gait recognition system: deep dive into this future tech,* recfaces.com blog post, https://recfaces.com/articles/what-is-gait-recognition

identify the people walking through their doors. It has become virtually impossible for people to move through the United States without being watched.

Federal Trade Commission Complaints. Over the last few years, the FTC has received numerous complaints against location data brokers who are collecting and selling the location information on hundreds of millions of people. A review of five of the complaints filed by the FTC reveals common business practices among location data brokers, among them:

- Brokers amass and sell raw location data that tracks consumers' movements so that their customers can glean insights into the consumers' private lives.

- Brokers also use the data to identify consumers based on attributes and behaviors the data reveals, including sensitive and personal attributes and behaviors, and they disclose the information to their customers.

- Brokers do not collect mobile location data directly from consumers. Generally, location brokers obtain location data from other data brokers. Those brokers, in turn, obtain data from other brokers, the mobile advertising marketplace, or mobile applications.

- For the most part, consumers have no interactions with brokers and have no idea that they have obtained their location data.

- Once the information is collected, it can be sold multiple times to companies that the consumer has never heard of, and the consumers have no insight into how this data is used and the associated risks. Because of the opaque nature of this industry, consumers are unable to take any reasonable steps to contain their data.

- The data collected is not anonymized, making it possible to identify the mobile device owner by combining the consumer's geolocation data and the mobile device's mobile advertising ID, which are alphanumeric identifiers that operating systems assign to each mobile device.

Mobilewalla, Inc. This company claims that it collects 50 billion mobile signals a day from 2.2 billion devices for 40 countries and stores over five years' worth of data. This broker touts its ability to "create a comprehensive, cross channel view of the customer, understanding online and offline behavior." Mobilewalla estimates that it collected more than 2 billion unique advertising identifiers between 2018 and 2020. According to a March 2020 email from the company's CEO obtained by the FTC, the company can identify consumers' home addresses using a consumer's mobile device location history and it is more accurate than its competitors because of their ability to store more data. Mobilewalla claims it can target geolocation to a radius as small as 25 meters (approximately 82 feet). [28]

The company has used sensitive information to create audience segments that helped clients target pregnant women, Hispanic churchgoers, and members of the LGBTQ+ community. It has created geo-fences around pregnancy centers and maternity clinics; created retroactive geo-

[28] 202-2196 In the Matter of Mobilewalla, Inc. United States Federal Trade Commission.

fences around the sites of political rallies and protests; and geo-fenced polling places and state capitols to identify devices belonging to consumers who visited those locations and identifying home addresses found within the geo-fence by tracking where the individuals spend the evening. For one client Mobilewalla created a geo-fence around the home addresses of a set of employees and certain healthcare centers, in order for the client to "poach these nurses from these centers to a competitor." Finally, in other non-advertising activities, it attempted to geo-fence a work location to track where union organizers travel.[29]

Kochava, Inc. According to FTC court filings, this location broker sold data that allows entities to track individuals' movements from sensitive locations, including locations associated with medical care, reproductive health, religious worship, mental health, and domestic violence shelters. The company claims that its location data feed delivers latitude/longitude data of around 94 billion geo transactions per month, 125 million monthly active users, and 35 million daily users, on average observing more than 90 daily transactions per device."[30]

The company has sold access to its data feeds on publicly accessible online marketplaces. It typically charges a monthly subscription fee of thousands of dollars to access its data feed, but it also offers a free sample of a subset of the paid data feed for a rolling seven-day period. According to the FTC, in just using the data sample it was possible to identify a mobile device that had visited a women's reproductive health clinic and trace that device to a single-family residence. The data set also revealed that the same device was at a particular location at least three evenings in the same week, suggesting the device user's routine. The sample data also identified a device that appears to have spent the night at a temporary shelter for at-risk, pregnant young women or new mothers.[31]

VI. HOME SURVEILLANCE SYSTEMS

Home surveillance cameras may seem like a helpful and innocuous security tool. However, there are significant tradeoffs in terms of Californians' privacy. The technology captures the movements of people both in public and in their homes on recorded and live video feeds that can be accessed by hackers, the companies making the technology, and by law enforcement officials.

Home security systems that include facial recognition, facial detection, and automobile detection can be purchased on Amazon for less than $500. Similarly, doorbells and door locks using facial recognition and other biometric data are available for around $200. All this biometric data that is captured needs to be stored and, depending on the companies' terms and conditions, could potentially wind up in a commercial database that may be accessed by data brokers and others, revealing the identity and location of any individual who passes by those security cameras.

Not only does the proliferation of these devices increase government surveillance, it also greatly increases the ability for individuals to hack into the cameras to gain access to private videos. In

[29] *Ibid.*
[30] *Federal Trade Commission v. Kochava, Inc*., 2:22-cv-00377, (D. Idaho).(Aug. 12, 2022) https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc
[31] *Ibid.*

May 2023, the FTC issued a consumer alert warning people that these systems presented a privacy risk. According to the alert:

> The FTC says Ring's poor privacy and lax security let employees spy on customers through their cameras, including those in their bedrooms or bathrooms, and made customers' videos, including videos of kids, vulnerable to online attackers. Hackers exploited those vulnerabilities and harassed, insulted, and propositioned children and teens through their Ring cameras. Some hackers even live streamed customers' videos.

Ultimately, Ring settled the case by agreeing to delete the videos that they should not possess, establish a privacy and security program, and pay $5.8 million to affected customers.[32]

In a recent investigation, Consumer Reports warned that video doorbells can be easily hacked. According to the findings, video doorbells sold on websites for Walmart, Amazon, Temu, Sears, and Shein could be taken over by someone with physical access to the doorbells, who then creates an account on a smartphone app and pairs the doorbell with their phone. The individual can then become the "owner" of the doorbell and see who arrives and leaves.[33] This presents a serious risk to the privacy of anyone in the home. Perhaps more importantly, these technological weaknesses could endanger people who are victims of stalking or intimate partner violence who installed these cameras thinking that they add an additional layer of security.

The use of global positioning system (GPS) technology on phones and in cars, combined with a growing network of public and private surveillance cameras, including home security cameras, makes it increasingly unlikely that people can leave their homes without having their every movement tracked by private companies, their neighbors, and their government.

VII. WORKPLACE SURVEILLANCE

Over the last five years, surveillance tools have become more affordable and more intrusive. As with personal information in general, employers can collect vast dossiers on their employees, gathering sweeping amounts of data about every aspect of their jobs and personal lives. Often that is done "without employees' full informed or free consent. Many workers, while generally aware they are being monitored, don't know the extent of the surveillance or what is being done with the information."[34]

Employers are using more surveillance technology than ever — digital cameras, motion scanners, RFID badges, Apple Watch badges, Bluetooth beacons, keystroke logging — to track every single movement of workers in the office and to gauge their productivity. Some workplaces are using biometric data such as eye movements, body shifts, and facial expressions, captured by computer webcams, to evaluate whether their employees are being appropriately attentive in their work tasks. As an example, artificial intelligence (AI) systems at call centers

---

[32] Puig, Alvaro. *Ring's privacy failures led to spying and harassment through home security cameras.* FTC Consumer Advice (May 31, 2023) *available at* https://consumer.ftc.gov/consumer-alerts/2023/05/rings-privacy-failures-led-spying-and-harassment-through-home-security-cameras

[33] Higginbotham and Wroclawski. "These Video Doorbells Have Terrible Security. Amazon Sells Them Anyway." *Consumer Reports* (Feb 29, 2024) *available at* https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/

[34] *Ibid.*

record and grade how workers are handling calls. This technology can be used to "coach" workers while they are talking to customers, telling them to sound happier or be more empathetic.[35] Another example is wearable technology that, among other things, tracks a worker's movements throughout the day, gathering biometric data, measuring how many times they use the bathroom, how long they spend in break areas, and which employees are spending time together. At least one company sells biometric ID badges with microphones, sensors, and other tools to record conversations, monitor speech, body movements, and location.[36] Even body temperature, sweat, and frequency of bathroom visits can be tracked and analyzed by employers.

A recent article in *MIT Technology Review* describes one company's surveillance tool this way:

> Companies that use electronic employee monitoring report that they are most often looking to the technologies not only to increase productivity but also to manage risk. And software like Teramind[37] offers tools and analysis to help with both priorities. While Teramind, a globally distributed company, keeps its list of over 10,000 client companies private, it provides resources for the financial, health-care, and customer service industries, among others—some of which have strict compliance requirements that can be tricky to keep on top of. The platform allows clients to set data-driven standards for productivity, establish thresholds for alerts about toxic communication tone or language, create tracking systems for sensitive file sharing, and more.
>
> [. . .]
>
> Selecting and tuning the appropriate combination of data is up to Teramind's clients and depends on the size, goals, and capabilities of the particular company. The companies are also the ones to decide, based on their legal and compliance requirements, what measures to take if thresholds for negative behavior or low performance are hit.[38]

Case study: Amazon. Perhaps the most extreme example of the intrusive surveillance tools used by employers can be found at Amazon. According to documents filed by Amazon workers with the National Labor Relations Board, Amazon tracks every minute that their workers spend off of their tasks. To do this, they use handheld scanners that are also used to track packages. The worker claims they "can receive a written warning for accumulating 30 minutes of time off task in a day one time in a rolling one-year period. They can be fired if they accumulate 120 minutes of time off task in a single day or if they have accumulated 30 minutes of time off task on three separate days in a one-year period."[39] Counted among the activities considered "time off task" are going to the bathroom, talking to another worker, or going to the wrong workstation. Workers reported that they were afraid to go to the bathroom or get a drink of water for fear of

---

[35] Kevin Roose, "A Machine May Not Take Your Job, but One Could Become Your Boss," *New York Times* (Jun. 23, 2019) https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html
[36] Humanyze: The Future of Workforce & Market Intelligence https://humanyze.com/
[37] https://www.teramind.co/solutions/compliance-management/
[38] Rebecca Akermann, "Your Boss is Watching," *MIT Technology Review* (Feb. 24, 2025
[39] Lauren Kaori Gurley, "Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts" *Vice* (Jun. 2, 2022) https://www.vice.com/en/article/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts/

being disciplined.[40] At the end of each shift, supervisors are required to interrogate the worker with the highest time off task.

Along with the handheld devices, Amazon uses an AI camera system trained on each workstation analyzing workers' movements. The cameras automatically register the location of products and catalog every mistake workers make.[41] Monitoring the workers' non-stop labor also helps improve the AI computer system, which learns from the responses of Amazon's video reviewers and becomes more accurate over time.[42]

Oxfam, an international organization focused on fighting global poverty, investigated the workplace surveillance practices at Amazon and Walmart warehouses in the United States. Employers like Amazon often claim that their surveillance systems are designed to make workers safer. "However, in recent years worker groups have decried the high injury rates and horrific working conditions that workers encounter as Amazon employees."[43] The report describes the surveillance technology as follows:

> The scanners play a key role in the surveillance machine because what the scanner records can lead to "Associate Development and Performance Trackers," or "ADAPTs," which are automated write-ups that penalize workers for not meeting production goals. In addition, hundreds of security cameras are constantly monitoring the warehouse floor, ready to notify a manager when a worker is away from their station for too long.
>
> [. . .]
>
> Another example of the detailed metrics that Amazon monitors is a worker's units per hour (UPH) score, which records how many actions a worker is able to accomplish in an hour. . . . [W]orker metrics are prominently displayed on a monitor, which keeps workers psychologically primed to constantly worry about "making rate" and about how they are doing compared with their co-workers. . . . Importantly, workers are not told what the data that electronic devices are constantly collecting is being used for, nor are they properly notified of their privacy rights.

VIII. DANGERS ASSOCIATED WITH SURVEILLANCE CAPITALISM

Some may consider sharing their private information, including browser history, purchases, previous employers, menstrual cycles, name, pictures, locations and movements, social media posts and reactions, and other seemingly innocuous information a reasonable price to pay for freely accessing the internet. However, failing to protect our private information can have real world consequences. As an example, the dating app, Grindr, was fined 10 percent of its global annual revenue by the Norwegian Data Protection Authority in 2021 for sharing deeply personal

---

[40] *Ibid.*
[41] Niamh McIntyre and Rosie Bradbury, *The eyes of Amazon: a hidden workforce driving a vast surveillance system*, The Bureau of Investigative Journalism (Nov. 21, 2022) https://www.thebureauinvestigates.com/stories/2022-11-21/the-eyes-of-amazon-a-hidden-workforce-driving-a-vast-surveillance-system/
[42] *Ibid.*
[43] *At Work and Under Watch: Surveillance and suffering at Amazon and Walmart warehouse*, Oxfam (Apr. 10, 2024) https://www.oxfamamerica.org/explore/research-publications/at-work-and-under-watch/

information with advertisers, including location, sexual orientation and mental health details.[44] This was not the first privacy violation Grindr had committed. Several years earlier, it was revealed that the company had shared HIV status and the location data from their users with two companies who were contracted to optimize the Grindr platform.[45]

Surveillance capitalism brings with it a myriad of harms. It creates dossiers that can easily reveal a person's reproductive health needs and choices, a person's gender and whether they are seeking gender affirming care, and a person's country of origin and immigration status. In the current political environment, these dossiers can easily cause someone to be imprisoned or killed. Beyond those significant risks, as demonstrated earlier, surveillance capitalism can cause consumers to be manipulated into paying more than they may be able to afford for goods or services. In addition, it can have profound and dire consequences for those women who find themselves in an abusive relationship and for people serving in public office.

Stalking and Intimate Partner Violence. Statistically speaking, the most dangerous place for a woman is not out in public, it is in her home. The most dangerous people for a woman are not strangers, they are the men she knows and has relationships with (e.g. current and former partners, family members, and friends). When the danger is someone who lives in their home, survivors need a safe, quick means of escape. Adding to the risk, the most dangerous time for someone who is in a relationship with a violent abuser is when they decide to leave. Unfortunately, geotags (like Apple's Air Tags), smartphones, smartwatches, find my friend or find my device apps, and apps that are connected to automobiles make leaving that much more dangerous and complicated.

The rising dangers for people in relationships with violent perpetrators parallels technological advancements. Technology has brought new and inventive ways for perpetrators to inflict abuse. In fact, the federal government now recognizes technological abuse as a form of domestic abuse. The Office of Violence against Women housed in the US Department of Justice defines technological abuse as:

> An act or pattern of behavior that is intended to harm, threaten, control, stalk, harass, impersonate, exploit, extort, or monitor another person that occurs using any form of technology, including but not limited to: internet enabled devices, online spaces and platforms, computers, mobile devices, cameras and imaging programs, apps, location tracking devices, or communication technologies, or any other emerging technologies.[46]

A *New York Times* article in 2018 explored the relatively new phenomenon of abuse cases that were tied to smart home technology. According to the article, domestic violence shelters were reporting calls from women who were convinced they were going crazy. They reported that their air-conditioning systems turned on and off without them touching them, that the code numbers on front door digital locks changed daily and they could not figure out why, or that they kept

---

[44] Hern, Alex. "Grindr fined £8.6m in Norway over sharing personal information," *The Guardian* (Jan. 26, 2021) https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information.
[45] "Grindr shared information about users' HIV status with third parties." *The Guardian* (Apr. 3, 2018) https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.
[46] Information on the types of domestic violence and the Office of Violence against Women can be found at https://www.justice.gov/ovw/domestic-violence.

hearing the doorbell ring, but no one was ever there. Through over 30 interviews, the *Times* reported that:

> [D]omestic abuse victims, their lawyers, shelter workers and emergency responders described how the technology was becoming an alarming new tool. Abusers — using apps on their smartphones, which are connected to the internet-enabled devices — would remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power. Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse.[47]

Today, internet connected devices are even more commonplace. Abusers use connected devices to terrorize, stalk, and surveil their victims. Smart speakers can often be used to listen in on conversations through an online app. Home security cameras and baby monitors can allow an abuser to watch and record their victims. Small tracking devices can be easily hidden in bags, clothing, or vehicles, allowing an abuser to monitor their victim's movements. As each new technology seeps into everyday life, abusers have adopted and repurposed them to terrorize and control their current and former partners.

In 2012, General Motors' OnStar debuted Family Link, a service that allowed remote users to track their family members and receive alerts about where the car goes. In the intervening years, advocates and experts working with survivors of stalking and domestic abuse have warned about the dangers related to allowing this type of technology in cars without offering a way for it to discreetly be turned off by the driver.[48] Over the last 12 years, this technology has become more sophisticated and common with most new cars offering remote vehicle technology that allows anyone with a smart phone app to check a car's location, including following the movement of the car in real time, tracking the history of where the car has been driven to, locking and unlocking the vehicle remotely; turning it on or off; altering the car's climate controls, making the horn honk; and turning on the car's lights.[49]

Even if a woman has successfully left her abuser and protected her address through the Safe at Home address confidentiality program that allows state and local agencies to both accept and respond to requests for public records without disclosing her changed name or address, the ability of abusers to purchase location data directly from a data broker through a "people search" website means that survivors will never truly be safe.

Political Violence. On June 14, 2025, Vance Boelter, posing as a law enforcement officer, knocked on the door of Senator John Hoffman's home and shot him and his wife, Yvette, over eight times. Boelter then drove to two other elected officials' homes that were empty before arriving at Representative Melissa Hortman's home, where he shot and killed her and her

---

[47] Bowles, Nellie. "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," *The New York Times* (Jun. 23, 2018) https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[48] Lineman, Tracey. "Connected Car Technology Can Enable Abusers to Track Their Victims," *Motherboard, Tech by Vice* (Aug. 14, 2018) *available at* https://www.vice.com/en/article/gy3kw7/internet-connected-car-technology-can-enable-abusers-to-track-victims.

[49] Hill, Kashmir. "Your Car Is Tracking You. Abusive Partners May Be, Too." *The New York Times* (Dec. 31, 2023) *available at* https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html.

husband, Mark. Once arrested, Boelter was found with a list of 45 elected Minnesota officials.[50] The list containing these officials' addresses allegedly came from data brokers and was obtained by Boelter using people search websites.[51]

Boelter's night of terror was just the latest in a string of alarming, politically motivated violence against elected officials. In July 2020, Daniel Anderl was home from college when attorney Roy Den Hollander knocked on the door. Hollander posed as a FedEx employee to gain access to the home of Judge Esther Salas, Daniel's mother. When Daniel answered the door instead of his mother, Hollander raised a firearm and shot and killed Daniel, leaving Mark Anderl, Daniel's father, critically injured as well.[52]

In 2022, former House Speaker Nancy Pelosi's home was broken into by a right-wing extremist who attacked her husband with a hammer. Several House Republicans claimed they experienced a barrage of threats and harassment in 2023 after voting against conservative Rep. Jim Jordan for speaker.[53] A 2024 report from the Brennan Center for Justice surveyed over 1,700 officials from across the country and found that more than 40 percent of state legislators experienced threats or attacks from 2021-2024, and over half experienced harassment such as stalking.[54] Officials who identify as women or people of color were more likely to experience threats and harassment related to their families, including threats against their children, than other officeholders. As a result, they were more likely to reconsider running for reelection due to these threats than men, highlighting how political violence could significantly reshape California's elected bodies.[55]

IX. PUBLIC/PRIVATE SURVEILLANCE PARTNERSHIPS

Adding to the complexity of our current surveillance state, the distinction between government surveillance and surveillance by private companies for profit has become blurred. Surveillance in the U.S. has become a largely private endeavor where private-sector companies are conducting surveillance and sharing the spoils with law enforcement, often enabling law enforcement to forego seeking a warrant.

License plate readers. Automated License Plate Reader (ALPR) systems are searchable computerized databases resulting from the operation of one or more cameras combined with computer algorithms to capture and convert images of registration plates and the characters they contain into computer-readable data. The cameras can be mobile, e.g., mounted on patrol cars, or

---

[50] Kevin Shalvey and Emily Shapiro, "Chilling details emerge in Minnesota shootings as Vance Boelter faces federal charges: 'Stuff of nightmares.' *ABC News* (June 16, 2025), https://abcnews.go.com/US/minnesota-lawmakers-shooting-suspect-vance-boelter-due-court/

[51] Lily Hay Newman, "Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets' Addresses." *Wired* (June 16, 2025), https://www.wired.com/story/minnesota-lawmaker-shootings-people-search-data-brokers/.

[52] William K. Rashbaum, "Misogynistic Lawyer Who Killed Judge's Son Had List of Possible Targets," *The New York Times,* (July 25, 2020), https://www.nytimes.com/2020/07/25/nyregion/roy-den-hollander-esther-salas-list.html

[53] David Li and Mirna Alsharif, "David DePape, man who attacked Paul Pelosi with a hammer, sentenced to 30 years in prison" (May 17, 2024), https://www.nbcnews.com/news/us-news/david-depape-man-attacked-paul-pelosi-hammer-sentenced-30-years-prison-rcna152614; and Lauren Peller, Rachel Scott, and Benjamin Siegel, "Republicans who voted against Jordan for speaker say they've been threatened, harassed" ABC News (October 19, 2023) https://abcnews.go.com/Politics/republicans-voted-jordan-speaker-threatened-harassed

[54] Gowri Ramachandran et al., *Intimidation of state and local officeholders* (Brennan Center for Justice, 2024), https://www.brennancenter.org/our-work/research-reports/intimidation-state-and-local-officeholders

[55] Ramachandran et al, *Officeholder intimidation,* 17.

fixed, e.g., mounted on light poles. ALPR systems allow for the widespread and systematic collection of license plate information. ALPR data can have legitimate uses, including for law enforcement purposes.

A recent investigation into the Flock Safety ALPR system by *404 Media*, an independent media company that specializes in technology, found more than 4,000 nation and statewide lookups by local and state police nationwide done either at the behest of the federal government or as an informal favor to federal law enforcement, or with a potential immigration focus.[56] According to the report:

> "Law enforcement really likes license plate readers because of the lack of restrictions on that data. They don't feel like they need a warrant. Oftentimes there are no restrictions whatsoever on what they search," Dave Maass, who studies border technology at the Electronic Frontier Foundation, told 404 Media. "It might be totally true that some of these searches are for people who have warrants or who are wanted for criminal activity. They might be looking for a terrorist, who knows. But that's kind of the point—we don't know."[57]

In an extension of their research, *404 Media* found that law enforcement authorities in Texas performed a nationwide search of over 83,000 Flock ALPR cameras in a search for a woman who they claim had a self-administered abortion. The article notes:

> The news shows in stark terms how police in one state are able to take the ALPR technology. . . . and turn it into a tool for finding people who have had abortions. In this case, the sheriff told 404 Media the family was worried for the woman's safety and so authorities used Flock in an attempt to locate her. But health surveillance experts said they still had issues with the nationwide search.[58]

The search by the officer logged the reason as "had an abortion, search for female."[59] Ashley Emery, senior policy analyst in reproductive health and rights at the National Partnership for Women & Families, told *404 Media*:

> The risks of this intrusive government monitoring cannot be overstated: law enforcement could deploy this surveillance technology to target and try to build cases against pregnant people who travel for abortion care and those who help them. This incident is undeniably a harbinger of more AI-enabled reproductive surveillance and investigations to come. Especially for women of color who are already over-surveilled and over-policed, the stakes couldn't be higher.[60]

As for California, several lawsuits and investigations have revealed that some local law enforcement entities are routinely violating California laws against sharing ALPR data out of state and with the federal government, including U.S. Immigration and Customs Enforcement

---

[56] Koebler and Cox, *supra*.
[57] *Ibid*.
[58] Joseph Cox and Jason Koebler, "A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion," *404 Media* (May 29, 2025) https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/.
[59] *Ibid*.
[60] *Ibid*.

(ICE), which used the information to track and deport immigrants.[61] Examples include the Sheriffs in Marin, Orange, and San Diego Counties, and the Vallejo and Los Angeles police departments.[62,63]

Compounding this issue, Flock recently announced the launch of their new product *Nova*, which is being promoted as supplementing license plate data with a wealth of personal information sourced from other companies and the wider web. The tool will potentially link footage of vehicles to their owners and then more people connected to them. According to internal documents acquired by *404 Media*:

> "You're going to be able to access data and jump from LPR to person and understand what that context is, link to other people that are related to that person [. . .] marriage or through gang affiliation, et cetera," a Flock employee said during an internal company meeting, according to an audio recording. "There's very powerful linking." One Slack message said that Nova supports 20 different data sources that agencies can toggle on or off.
>
> [. . .]
>
> In the meeting audio obtained by 404 Media, the Flock employee described the sorts of information the company will supplement ALPR data with. The first is data breaches. One example the employee pointed to was a 2021 data breach impacting users of Park Mobile, an app that allows users to pay for parking without physically going to the parking meter or in some lots where meters no longer exist. That data included license plate numbers with their owners' associated email addresses, phone numbers, and in some cases mailing addresses. With regards to Flock, "Nova ingests that and is able to use that to contextualize the data. So we're now able to make that cognitive leap from LPR to person," the employee said.
>
> [. . .]
>
> The second was "commercially available data," with the employee explicitly naming credit bureaus Equifax and TransUnion. . . . [W]hen people open a credit card their personal information is sent to the credit bureaus in their role as monitoring peoples' credit. Some bureaus then repackage and sell this information to law enforcement or other data brokers. TransUnion has a data product called TLOxp. . . .
>
> The third is public records such as marriage licenses, property records, and campaign finance records, the employee said. The slides say that Nova will also pull data from law enforcement Records Management Systems (RMS), which are typically databases for storing

[61] Senate Bill 54, the California Values Act, which took effect on January 1, 2018 establishes statewide non-cooperative policies between state and local law enforcement officials and federal immigration authorities.
[62] Johana Bhuiyan, "How expanding web of license plate readers could be 'weaponized' against abortion," *The Guardian* (Oct. 6, 2022) https://www.theguardian.com/world/2022/oct/06/how-expanding-web-of-license-plate-readers-could-be-weaponized-against-abortion?ref=vallejosun.com.
[63] Khari Johnson and Mohamed Al Elew, "California police are illegally sharing license plate data with ICE and Border Patrol," *CalMatters* (Jun. 13, 2025) https://calmatters.org/economy/technology/2025/06/california-police-sharing-license-plate-reader-data/.

information on cases, and Computer Aided Dispatch (CAD) systems, which manage responses to 911 calls.[64]

Another company, Vigilant Solutions, has amassed billions of license plate records throughout the county that allow law enforcement officials to monitor the movements of individuals by linking the license plate records with facial recognition technology.[65] All of this information, potentially tracking people to sensitive locations, is available to any paying law enforcement agency.

Home security systems. In 2022, the city of San Francisco embarked on a citywide surveillance experiment that explicitly allows law enforcement to access the live footage of privately owned internet cameras without first obtaining a court order or warrant.[66] Prior to the passage of the local ordinance, law enforcement could request previously recorded footage from the owners of internet cameras or ask the surveillance technology companies for data, but they could not tap into the live feeds of privately owned cameras. As the technology becomes more readily available and other jurisdictions consider these types of ordinances, the ability for law enforcement to tap into real-time private video feeds through the owners of the systems and the technology companies could become increasingly commonplace.

During the recent 60th Super Bowl performance, Ring released a 30-second ad about their new feature Search Party, which allowed a young girl to find her missing dog by connecting to other Ring doorbell cameras in the neighborhood. Jamie Siminoff, Ring's founder, proclaimed in the ad: "[b]e a hero in your neighborhood with Search Party" as he strolled through an idyllic suburban neighborhood. The backlash was swift.[67] The jump from surveilling the neighborhood for a missing dog to surveilling people was obvious for some, with YouTube comments for the ad referencing "dystopian" futures and doubting whether the intent of Search Party extended only to finding lost dogs.[68] In fact, internal emails from the company reveal that Siminoff's plans for Search Party went beyond finding missing dogs. In October, Siminoff emailed all Ring employees that the new feature would soon be able to "zero out crime in neighborhoods."[69]

This is not the first time that Ring, which was bought by Amazon in 2018 has drawn public ire. In the late 2010s, Ring faced criticism for having over 600 partnerships with police and hosting

---

[64] Joseph Cox, "Flock Is Building a Massive People Lookup Tool, Leak Shows," *404 Media* (May 14, 2025) https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/.

[65] https://www.ra-comm.com/vigilant-solutions/

[66] *News Release - Board of Supervisors Approves Camera Access Legislation to better Protect Residents, Businesses, and Neighborhoods*. Office of the Mayor (Sep 21, 2022) *available at* https://sfmayor.org/article/board-supervisors-approves-camera-access-legislation-better-protect-residents-businesses-and

[67] Jordyn Holman, "Ring's Founder Knows You Hated That Super Bowl Ad," *The New York Times,* (Feb 19, 2026), https://www.nytimes.com/2026/02/19/business/ring-super-bowl-ad-privacy.html

[68] Jason Koebler, "With Ring, American Consumers Built a Surveillance Dragnet," *404 Media,* (Feb 10, 2026), https://www.404media.co/with-ring-american-consumers-built-a-surveillance-dragnet/?ref=daily-stories-newsletter

[69] Jason Koebler, "Leaked Email Suggests Ring Plans to Expand 'Search Party' Surveillance Beyond Dogs," (Feb 18, 2026), https://www.404media.co/leaked-email-suggests-ring-plans-to-expand-search-party-surveillance-beyond-dogs/?ref=daily-stories-newsletter

elaborate parties for law enforcement.[70] In October 2025, Ring announced a partnership with Flock Safety, the ALPR company discussed above..[71] The partnership was an extension of the Community Request feature, which allowed law enforcement agencies to request footage and information from Ring customers about reported crimes by 'pinging' them on the Ring feed. The Flock partnership was intended to empower communities to engage with public safety. "The expansion of Community Requests will empower more communities to do what they've always wanted to do – help."[72]

Immigration and Customs Enforcement's partnership with private surveillance companies. Flock has faced a litany of complaints from the public and privacy experts alike for sharing their data with not only law enforcement but with ICE agents.[73] The company has also been criticized for serving as a tool to surveil protected actions such as demonstrations without critical oversight (officers rarely need a search warrant to use Flock, making it hard to track and monitor when Flock is being accessed and for what purpose).[74] Following the Super Bowl ad backlash, Ring cancelled their partnership with Flock.[75]

Notably, there is no evidence that Ring's camera footage is accessible to ICE.[76] However, the backlash highlights a rising trend in the public's awareness of commercial surveillance tools falling into the hands of federal agents. Several cities and municipalities have pulled their contracts or tightened their data-sharing clauses with Flock following rising public scrutiny surrounding ICE's ability to access the license plate readers.[77]

The data analytics platform Palantir services federal, state, and local agencies. Palantir has profited significantly by partnering with the current federal administration to provide surveillance tools such as ImmigrationOS, which provides real-time updates on immigrants self-deporting from the US,[78] and Enhanced Leads Identification & Targeting for Enforcement (ELITE), which creates maps of potential deportation targets using Department of Homeland

[70] Caroline Haskins, "'FUCK CRIME:' Inside Ring's Quest to Become Law Enforcement's Best Friend," *Vice,* (Dec 4, 2019), https://www.vice.com/en/article/inside-rings-quest-to-become-law-enforcements-best-friend/?ref=404media.co
[71] Ring, "Ring Expands Community Requests to Additional Community Safety Partners," (Oct 16, 2025), https://blog.ring.com/about-ring/ring-expands-community-requests-to-additional-community-safety-partners'/
[72] Ibid.
[73] Jason Koebler & Joseph Cox, "ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows," *404 Media,* (May 27, 2025), https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/
[74] Dave Maass & Rindala Alajaji, "How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists," *Electronic Frontier Foundation,* (Nov 20, 2025), https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists
[75] Annie Palmer, "Amazon's Ring cancels Flock partnership amid Super Bowl ad backlash," *CNBC,* (Feb 12, 2026), https://www.cnbc.com/2026/02/12/amazons-ring-cancels-flock-partnership-amid-super-bowl-ad-backlash.html?msockid=2e95daf716196a46331fcc2d17706b33
[76] Jon Chase, "Ring Denies Rumors That Its Footage Is Used by ICE. Here's What to Know." *Wirecutter,* (Feb 13, 2026), https://www.nytimes.com/wirecutter/reviews/ring-cameras-ice-what-to-know/
[77] Jude Joffe-Block, "Why some cities are ditching their Flock license plate readers," *NPR,* (Feb 19, 2026), https://www.npr.org/2026/02/17/nx-s1-5612825/flock-contracts-canceled-immigration-survillance-concerns
[78] Caroline Haskins, "ICE Is Paying Palantir $30 Million to Build 'ImmigrationOS' Surveillance Platform, *Wired,* (Apr 18, 2025), https://www.wired.com/story/ice-palantir-immigrationos/

Security (DHS) and the Department of Health and Human Services (HHS) data.[79] Palantir and DHS reached a $1 billion purchasing agreement in February 2026.[80]

Palantir has faced pushback for their involvement in ICE arrests. After the fatal shooting of Alex Pretti in Minneapolis, Palantir employees flooded their Slack Channel, asking for clarification and accountability about Palantir's contracts with DHS.[81] Palantir's CEO, Alex Karp, addressed concerns in a video but did not speak to how Palantir was supporting ICE, or the products that Palantir provides to ICE.[82] However, a video of an apparent ICE agent scanning a legal observer's car and saying, "[w]e have a nice little database, and now you're considered a domestic terrorist" has led some to speculate that Palantir may be providing this database for federal agents.[83] Palantir has not responded to questions about the database from reporters or from their own employees.

Federal contracting records reveal that ICE is planning to partner with private vendors to complete a surveillance program that scours Facebook, Tiktok, Instagram, Youtube and other platforms for data on individuals' social media activity.[84] This social media surveillance program would cast a wide net across the platforms, potentially catching not only undocumented individuals, but also those who express dissent with ICE's tactics at large.[85]

In September 2025, ICE lifted a stop-work order on a $2 million deal with the spyware company Paragon Solutions that develops spyware capable of hacking phones to monitor, track, and extract data.[86] The work order had been paused due to concerns that it violates a 2023 executive order limiting U.S. procurement of spyware.[87] Paragon has been implicated in widespread misuse by the Italian government, who used the spyware to surveil journalists and humanitarian

[79] Caroline Haskins & Makena Kelly, "ICE Is Using Palantir's AI Tools to Sort Through Tips," *Wired,* (Jan 28, 2026), https://www.wired.com/story/ice-is-using-palantirs-ai-tools-to-sort-through-tips/
[80] Makena Kelly, "DHS Opens a Billion-Dollar Tab With Palantir," *Wired,* (Feb 19, 2026), https://www.wired.com/story/department-homeland-security-ice-billion-dollar-agreement-palantir/?utm_source=nl&utm_brand=wired&utm_mailing=WIR_Daily_022026_UNPAID&utm_campaign=aud-dev&utm_medium=email&utm_content=WIR_Daily_022026_UNPAID&bxid=640b75831d57ae1d460eb8aa&cndid=73174143&hasha=2250b0ee2e84c60fb682ba09a91c346a&hashc=c731209aadca76c4664b1bff6d6ad6330ceef6257bfa4e4ee3631f9a10a3e85e&esrc=register-page&utm_term=WIR_DAILY_UNPAID
[81] Makena Kelly, "Palantir Defends Work With ICE to Staff Following Killing of Alex Pretti," *Wired,* (Jan 26, 2026), https://www.wired.com/story/palantir-ice-dhs-alex-pretti-killing-workers-slack-minneapolis/
[82] Makena Kelly, "Palantir CEO Alex Karp Recorded a Video About ICE for His Employees," *Wired,* (Feb 10, 2026), https://www.wired.com/story/palantir-ceo-alex-karp-employee-questions-on-ice/
[83] Makena Kelly, "Palantir Defends Work With ICE."
[84] Dell Cameron, "ICE Wants to Build Out a 24/7 Social Media Surveillance Team," *Wired,* (Oct 3, 2025), https://www.wired.com/story/ice-social-media-surveillance-24-7-contract/
[85] Sam Biddle, "ICE Wants to Know if You're Posting Negative Things About It Online," *The Intercept,* (Feb 11, 2025), https://theintercept.com/2025/02/11/ice-immigration-social-media-surveillance/
[86] Cooper Quintin, "EFF Statement on ICE Use of Paragon Solutions Malware," *The Electronic Frontier Foundation,* (Sep 3, 2025), https://www.eff.org/deeplinks/2025/09/eff-statement-ice-use-paragon-solutions-malware
[87] Jack Poulson, "Exclusive: ICE reactivated its $2 million contract with Israeli spyware firm Paragon, following its acquisition by U.S. capital," *Substack,* (Sep 1, 2025), https://jackpoulson.substack.com/p/exclusive-ice-has-reactivated-its

workers.[88] Three House Democrats sent a letter to DHS demanding more insight into the contract,[89] and *404 Media* is suing ICE for access to the contract.[90]

Another surveillance company, Penlink, struck a partnership with ICE to deploy surveillance tools that are "designed to monitor a city neighborhood or block for mobile phones, track the movements of those devices and their owners over time, and follow them from their places of work to home or other locations."[91] These contracts that ICE is striking often cost millions and allow them to bypass Fourth Amendment protections and other laws meant to protect privacy. Nowadays, the federal government can know nearly everything there is to know about any individual, from what celebrities they're following on social media, to what they gossip about with their friends, to their exact geolocation, all because the cell phone in their pocket allows private surveillance companies to scrape their data and sell it to the highest bidder, who may just be the federal government.

X. POLICY CONSIDERATIONS

Is California's judicial oversight of law enforcement surveillance adequate? Fourth Amendment jurisprudence requires a warrant before searching an electronic device or seeking information from an electronic communications provider.[92] Consistent with these principles, the California Electronic Communications Privacy Act generally prohibits government entities from obtaining electronic communication or device information without a legal order, except in cases involving emergencies, consent of the device owner, or abandonment of the device.[93] Given the ease with which law enforcement entities can partner with private vendors to surveil individuals, the question arises whether such protections should be strengthened. These issues are in the primary jurisdiction of the Public Safety Committee, the Chair of which has been invited to attend this hearing.

The challenge of an opt-out framework. The general framework for California's privacy laws focus on the idea that personal information can be collected, used, sold and shared if a person provides informed consent. The overwhelming majority of California's privacy laws are based on the idea of providing individuals with the right to "opt out" of having their personal information, including sensitive information such as immigration status, sexual orientation, and social security numbers, shared or sold. This approach, in effect, means that surveillance, rather than privacy is the default in California.

Publicly available information and privacy in public spaces. A major problem with US privacy laws, including California's, is its continued embrace of the belief "that anything exposed to the

---

[88] Stephanie Kirchgaessner & Angela Giuffrida, "European journalists targeted with Paragon Solutions spyware, say researchers," *The Guardian,* (Jun 12, 2025), https://www.theguardian.com/media/2025/jun/12/european-journalists-targeted-with-paragon-solutions-spyware-say-researchers

[89] Tim Starks, "House Dems seek info about ICE spyware contract, wary of potential abuses," *Cyberscoop,* (Oct 6, 2025), https://cyberscoop.com/house-dems-seek-info-about-ice-spyware-contract-wary-of-potential-abuses/

[90] Joseph Cox et al., "We're Suing ICE for Its $2 Million Spyware Contract," *404 Media,* (Sep 22, 2025), https://www.404media.co/were-suing-ice-for-its-2-million-spyware-contract/

[91] Joseph Cox, "Inside ICE's Tool to Monitor Phones in Entire Neighborhoods," *404 Media,* (Jan 8, 2026), https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/

[92] *See US v. Jones* (2012) 132 S.Ct. 945; *Riley v. California* (2014) 134 S.Ct. 2473.

[93] Pen. Code § 1546.1.

public, or data available to the public, or even information shared with others lacks any privacy interest because it is not totally secret. This flawed understanding of privacy creates two common and severe limitations of privacy law—a failure to protect privacy in public or publicly-available data."[94]

As Professor Daniel Solove notes, "most people do not live like hermits; they engage in their life's activities in places where other people congregate. People expect that their activities are private because they are obscure – others won't be paying attention or watching or listening."[95] As demonstrated throughout this paper, modern surveillance technologies have eroded this sense of obscurity. Contributing to the erosion of any semblance of privacy in public spaces is the notion that information that is "publicly available" is no longer private and becomes fair game. Most laws, including California's privacy laws, exempt from their protections "publicly available" information. In the CCPA, "publicly available" is broadly defined as any of the following:

- Information that is lawfully made available from federal, state, or local government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media.
- Information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.[96]

As Professor Solove warns:

> Companies are scraping vast quantities of personal data from the internet. . . . Scrapers argue that public information is fair game, and many privacy laws permit scraping by excluding publicly available data from their protections. The principle of obscurity, however, emphasizes that just because data is publicly accessible does not mean privacy is forfeited. Although the information may not be secret, its obscurity imposes significant limits on accessibility. Collecting personal data and making it easily discoverable fundamentally alters the level of privacy associated with that information.[97]

He urges policy makers:

> Rethinking the notion of publicly available information would close a gaping hole in privacy protection; it would prevent companies and the government from vacuuming up vast quantities of personal data; it would protect personal data online with important privacy safeguards and limitations.[98]

[94] Solove (2025)
[95] *Ibid.*
[96] Civ. Code § 1798.140(v)(2)(B).
[97] Solove (2025)
[98] *Ibid.*