UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

SCHOOL OF INFORMATION
102 SOUTH HALL # 4600
BERKELEY, CALIFORNIA 94720-4600
(510) 642-1464
www.ischool.berkeley.edu

Testimony of UC Berkeley Professor Deirdre Mulligan Before the California Assembly Committee on Privacy and Consumer Protection

March 03, 2026

Chair Bauer-Kahan and Members of the Committee, thank you for the opportunity to testify today. I am a Professor in the School of Information at UC Berkeley and a faculty Director of the Berkeley Center for Law & Technology. My research explores legal and technical means of protecting values such as privacy, freedom of expression, and fairness in socio-technical systems. My book, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, a study of privacy practices in large corporations in five countries, conducted with UC Berkeley Law Prof. Kenneth Bamberger, published in 2015 by MIT Press, was the first comparative study of corporate privacy work under different regulatory conditions and received the 2016 International Association of Privacy Professionals Leadership Award. During the Biden-Harris Administration I was honored to serve as Principal Deputy U.S. Chief Technology Officer at the White House Office of Science and Technology Policy, and Director of the National Artificial Intelligence Initiative Office (NAIIO) where I led the Technology Team that worked to advance technology and data to benefit all Americans. Beyond my scholarship, much of my service has revolved around protecting the public's privacy, including serving as: an inaugural board member of the Partnership on AI; a founding member of the Global Network Initiative, a multi-stakeholder initiative to protect and advance freedom of expression and privacy in the ICT sector; as a Commissioner on the Oakland Privacy Advisory Commission; and as chair of a series of interdisciplinary visioning workshops on Privacy by Design with the Computing Community Consortium to develop a shared interdisciplinary research agenda. Prior to joining the School of Information I was a Clinical Professor of Law, founding Director of the Samuelson Law, Technology & Public Policy Clinic, and Director of Clinical Programs at the UC Berkeley School of Law. Before coming to academia, I helped found the Center for Democracy and Technology, a leading advocacy organization protecting global online civil liberties and human rights.

In 2012, Target's data science team built a model that predicted a teenage customer's pregnancy from purchasing patterns, before the customer had told anyone, including her own family. Her father received targeted maternity coupons addressed to his teenage daughter and complained to the store, only to later learn that his daughter was in fact pregnant. That example is more than a decade old, and involved a relatively simple computational model applied to a relatively narrow set of purchasing data.

Three key changes over the past two decades have produced a new economic order, surveillance capitalism, in which human experience itself has become raw material for extraction, prediction, manipulation and sale by and for private profit:

First, the surveillance infrastructure has expanded. In the 1990s the birth of the commercial internet gave rise to unique concerns about the consumer protection, privacy and security implications of the pervasive and persistent digital footprints created by every online interaction. Today, the pervasive data collection associated with the Internet permeates our physical environment, as our physical world is becoming increasingly instrumented. Brick and mortar stores, no longer satisfied with register data, deploy technology including eye tracking software and facial recognition technology to monitor customers. And during COVID many stores moved away from accepting cash, encouraging and in some instances requiring customers to pay with credit cards or touchless apps that reveal purchasers' identity and store transaction data. Workplaces and even workers are increasingly instrumented with sensors–from key cards, to video surveillance, to eye tracking software, to wearables–that generate digital data. And the rise of AI enabled digital assistants and connected devices from watches to cars provide companies with windows into homes across the country, offering companies unprecedented access to information about mundane and intimate domestic activities and concerns. In addition, the near ubiquity of cell phones and smart phones combined with the rise of location based services has created a continuous stream of geospatial data revealing peoples movements through both public and private spaces. Surveillance is no longer episodic or confined to particular contexts, but ambient and embedded in the architecture of daily life.

Second, the variety and amount of data collected on individuals has grown. Companies that once collected purchase data, and in the digital environment behavioral data now collect biometric data–fingerprints, facial geometry, retina scans, voiceprints, gait, and DNA. The rise of social media exposed individuals' networks of friends, coworkers, acquaintances, fans and followers. These social graphs both explicitly and implicitly reveal information about individuals' interests, associations, beliefs, and facets of their identity. . The rise of LLM Chatbots has turbo charged the quantity and changed the quality of information individuals share with AI companies. Short search queries have been replaced by long form questions, and extended conversations vastly increase the amount of information shared with the private sector. And as individuals turn to chatbots for emotional support, spiritual guidance, relationship counseling, legal advice, business advice and in a growing number of instances intimacy, they are turning over reams of information about their follies, fantasies, neuroses, desires, hopes and fears, in ways that have no precedent in the history of commercial data collection.

Third, powerful advances in computation expand what private companies can glean from these troves of personal data. The machine learning and AI models available today can extract patterns and draw inferences about a wide range of topics from seemingly innocuous data. For example, health conditions or propensities can be inferred from nonmedical data generated far outside the medical context. In the Target story I opened with, the company inferred pregnancy from the purchase of a few non-pregnancy specific items–unscented lotion, vitamins–but researchers have shown that more powerful computational techniques can make more startling and category-jumping inferences, including those that reveal attributes or conditions an individual has specifically withheld from others. These advances in inference make it difficult for individuals to reason about the risks of disclosing information.

Taken together these three changes challenge two core assumptions of most U.S. privacy laws:

Existing privacy laws built around notice and consent, assume individuals are aware of and have a say over the collection of their personal data. The infrastructuring of physical spaces has pushed data collection behind the scenes and often outside of individuals' control. A person's presence in a physical space–a workplace, a public street, a commercial store–routinely subjects them to surveillance often without their knowledge and almost always without meaningful consent. In personal homes and on public streets, the Internet of Other people's things extracts data from individuals based on other

people's preferences. Surveillance has become the background condition of everyday life rather than an episodic event brought to an individuals' attention and over which they might be afforded some control.

Existing privacy laws, built around notice and consent at the moment of data collection, assume individuals understand the risks posed by disclosing different kinds of personal information because they understand what it reveals about them–i.e. they assume individuals understand the *meaning* of their data. In other words, privacy laws in the United States generally assume that the semantics of data are relatively fixed and knowable at the time of disclosure. But armed with sophisticated and powerful machine learning algorithms, companies (and governments) can draw powerful and compromising inferences from seemingly benign data making it increasingly difficult for individuals to understand the meaning, let alone the risks of disclosing any piece of their data. In this asymmetric environment, individuals' ability to control who knows what about them cannot be fully protected by notice and consent mechanisms focused on data collection.

Existing privacy laws generally assume that a person's data has implications for them but not others. Privacy operates at the individual level, but surveillance operates at the collective level. It leverages individuals' data to classify, make inferences and predictions, and manipulate not only them but others. Addressing the risks of surveillance capitalism requires strategies that operate and protect against risks posed by tranches of personal data, not just our own.

The rise of surveillance capitalism also lays bare the limits of viewing the stakes of sweeping population surveillance as solely a problem for individual privacy. Privacy is both an individual right and a public good. It affords individuals the space and freedom to learn and grow, form intimate relationships, worship, and form the independent opinions and perspectives essential to thriving democracies. It is a necessary bulwark against government and corporate power.

As the speakers on both of today's panels will describe in detail, the harms flowing from surveillance capitalism go well beyond intrusions on individuals' privacy. Surveillance capitalism is fueling unfair practices in the marketplace and the workplace.

- Companies use the surveillance infrastructure to generate individual prices for goods and services aimed at maximizing the revenue they can eke out of each individual consumer. They are weaponizing the public's personal information to make them poorer–extracting Californian consumers' hard earned wealth.

- Companies use the surveillance infrastructure as a living lab, seeking new methods to shape consumers' desires and behaviors, stealing our attention, influencing our health and well being. Gone are the days when you were paid to be a Nielsen family or part of brand research. Today, the digital infrastructure allows companies to run continuous experiments in the wild without notice, consent or participation.

- Employers use the surveillance infrastructure to classify and manage workers creating risks for workers' jobs, physical and mental health, privacy and civil rights, and at times interfering with employees' abilities to engage in collective bargaining and other protected activities.

And while this first panel is focused on surveillance capitalism, the private sector infrastructure and the pools of data and inferences it creates are of great interest to state actors both at home and abroad and the walls between the public and private sectors have become increasingly thin. Governments', particularly those acting lawlessly, share the private sector's interest in keeping individuals'--and populations'--behavior, associations, transactions, and identities articulated,

measurable, mineable and programmable. At this moment, as the public's data is being weaponized against them we can not ignore the risks private sector surveillance capitalism poses for the people as polity, not just consumers.

Surveillance capitalism imperils our shared commitment to constraining our government from overreaching surveillance of the US population, and it also poses threats to our national security. Other panelists will describe the risks to individuals' physical and mental health and security posed by surveillance capitalism. But, the rampant collection, sale and use of personal data poses collective risks. The connection between the availability of the American publics' personal data and national security is a growing concern. Access to Americans' personal data, from data brokers and other sources, increases the ability of malicious actors–from foreign adversaries, to extortionists–to engage in a wide range of activities that threaten our collective and indeed national security: from coercion and manipulation of specific employees; to ransomware and other attacks on high value systems including schools, hospitals and public agencies; to influence campaigns seeking to alter elections or sow domestic turmoil. In addition, personal data linked to populations and locations associated with the Federal Government—including the military—can be used to reveal insights about those populations and sensitive locations that threaten national security. Surveillance capitalism–its infrastructure, the data it produces, the inferences it learns–provide assets and strategic advantages to those seeking to attack our infrastructure, manipulate our population, or undermine the trust and stability of our government. Put simply, surveillance capitalism threatens not only individual privacy and security but our collective safety and security.

I offer a few recommendations to move us in this direction:

First, protecting the collective, public, and social value of privacy requires policy makers to refocus on addressing the collective harms, as well as individual ones, that flow from surveillance practices. These harms expand beyond those construed as privacy (too often reduced to information control) as they rest in the power of personal data in identifiable, aggregate and even deidentified forms to shape markets, preferences and societies. Public policy must contend with the role data and algorithms play in actively mediating and normalizing the discourses and social conditions against which decisions about distributions of power, resources and opportunities take place. Legislators must approach the regulation of personal data with the full range of human rights, consumer protection, competition, health, safety and security issues in view.

Second, focus on institutions and professionals, not just new rules. Our existing regulatory and enforcement agencies are understaffed and under-resourced to meet the challenges consumers are facing, and they need more sociotechnical experts to ensure they can accurately assess both the potential of and risks associated with technological advancements. Efforts must be dedicated towards building capacity commensurate with the technical sophistication of this problem, with active attention paid towards expanding technical staff and ensuring agencies have access to independent economic, engineering, data science, design, social science and other relevant expertise. This interdisciplinary expertise is fundamental to ensuring that lawmakers and enforcement agencies fully understand the surveillance ecosystem, the wide variety of harms it contributes to, and the range of interventions to address them.

Third, legislators should focus on the relations between the private sector and the government's acquisition of data. The growth of commercial surveillance infrastructure has reduced the practical constraints on state surveillance because government agencies can acquire vast amounts of personal data through donation, purchase or subpoena rather than warrant. This allows the state to leverage privately collected data to reconstruct movements, associations, and intimate activities. Even more forebodingly,

it can allow the state to tap into private surveillance systems in real-time, creating a flexibly deployable and wide reaching surveillance apparatus.

Finally, regulatory approaches that place the burden on consumers are impractical given the scale, invisibility, and ubiquity of devices and activities that collect data; the implications of other people's data and devices for the individuals privacy; and the increasingly powerful data analysis methods that are used to both understand and shape individuals and collective experiences and opportunities. Surveillance is a collective issue that implicates not just the information collected about an individual, but the information collected about their broader familial and social networks as well as the use of this information to in turn modify individuals' material and social conditions. Even when considering opportunities to empower individuals, regulations must consider the relevant contexts and asymmetries that would inform their calculus; for example, consent requirements are not meaningful if opting out forces individuals to opt out of the digital infrastructure that is essential to contemporary life. Overall, continuing to view this issue in a vacuum or as an individual responsibility may cause policy to miss the actual loci of harm.

As Principal Deputy Chief Technology Officer in the White House Office of Science and Technology Policy in the Biden-Harris Administration, I helped ensure that how we– both the government and private sector– designed, used, and regulated technology centered peoples' rights and freedoms, advanced equity, and adhered to our fundamental obligation to ensure fair and impartial justice for all. Today the world is looking to California to lead the way. How the Golden state uses, refuses and regulates technology is a key way that we manifest our values, including our California Constitutional right to privacy.