
CALIFORNIA PRIVACY PROTECTION AGENCY

400 R ST. SUITE 350
SACRAMENTO, CA 95811
cppa.ca.gov



INFORMATIONAL SESSION

**The Private to Federal Pipeline:
How Federal Agencies Use Private Data and How States Can Protect Americans**

April 30, 2026

OVERVIEW

This informational session will explore the collection of Americans’ personal information by the federal government, for example data purchased from data brokers, data transferred between government agencies, and data requests tied to immigration enforcement. The session will examine the existing commercial data flows and how the government acquires consumer data with limited oversight or restriction. It will also consider what existing privacy protections are available at the federal level, their effectiveness in the current political landscape, and the role states can play in protecting consumers.

AGENDA

I. Personal Information Data Flow Overview: How Is Personal Information Collected, Sold, and Shared with the Federal Government?

This session will examine data flows in today’s digital ecosystem. The panel will explore how certain types of data, like location data, can reveal an immense amount of private information about consumers. Panelists will explain how user data is collected by modern online service providers, apps, the advertising industry, and real-world surveillance and how that data is used and often even functionally necessary to deliver and improve services.

The session will also explore how consumer data then flows to the federal government. Panelists will discuss how user data is sold to the federal government through what is commonly known as the “data broker loophole,” and how AI supercharges the desirability of this commercially available information. The session will also explore how consumer data becomes a central resource for government investigations. Panelists will walk through the mechanics of legal demands for provider-held data in criminal and national security contexts, including the role of subpoenas, warrants, and various national security orders. Legal and public policy matters will be discussed, including the widespread use of secrecy orders, the important role of encryption, and the emerging use of artificial

intelligence.

The overall aim is to give a grounded account of how provider-held data moves from ordinary product use into investigative pipelines, and the legal and policy tensions that arise along the way.

II. Federal Access to Commercial Data: Existing Federal Framework and the Role of the States

This session will provide an overview of the privacy protections available at the federal level to protect consumers' commercial data from federal overreach. This panel will explore the role of the Federal Trade Commission (FTC) and existing protections available under the Federal Trade Commission Act, the Children's Online Privacy Protection Act, various FTC rulemakings, and cases brought by the FTC. The discussion will examine how concentration in marketplace can complicate enforcement and protections and how shifts in executive power and the independence of federal agencies may impact the protections available.

The session will also explore the role that states can play during a period of federal deregulation, including by discussing various options including data minimization standards, state enforcement of commercial practices, and private rights of action.

III. Federal Use of Commercial Data: Policy Approaches

This session will explore policy concerns related to the nonconsensual sharing of consumer data with law enforcement. Panelists will discuss how consumer data, collected under specific consumer expectations and then repurposed for government surveillance, can violate purpose limitation principles, create a chilling effect on lawful online activity, and disproportionately harm vulnerable communities. They will also explore the federal government's ongoing quest to consolidate and repurpose state-level administrative data, including attempts to demand Americans' personal data from third-party payment processors for programs like Supplemental Nutrition Assistance Program (SNAP), and the harms that creates for Americans.

The session will then review the legal tools currently available to address these problems, including the California Consumer Privacy Act and Delete Act, and how they can be used or strengthened to protect consumers. Panelists will discuss what additional regulatory guidance may be needed to minimize the sharing of consumer data with law enforcement and how the existing laws can be enforced to support consumers. Finally, the panelists will consider new policy proposals such as the federal Fourth Amendment Is Not for Sale Act and pending state bills.

SPEAKERS

Tom Bowman

Policy Counsel, Security & Surveillance, Center for Democracy and Technology (CDT)

Tom Bowman serves as Policy Counsel with CDT's Security & Surveillance Project, where he focuses on encryption, commercial spyware, reproductive and gender-affirming care, and law enforcement use of surveillance technologies. He represents CDT in numerous coalitions, including the Steering Committee of the Global Encryption Coalition, the Immigrant Surveillance Working Group, the Police Tech Working Group, and the Repro+Surveillance Privacy Hub.

Prior to joining CDT, Mr. Bowman worked as an assistant public defender at the Maryland Office of the Public Defender, where he represented clients facing misdemeanor and felony charges. He also interned at the Federal Public Defender for the District of Alaska. Earlier in his career, Mr. Bowman taught English in Bulgaria.

Mr. Bowman earned his B.S. in International Relations from the University of Iowa and his J.D. from NYU School of Law.

Jennifer Chen

Head of Operations, Good Research

Jennifer Chen oversees product and operations for Good Research's privacy and technical investigation work, including litigation and regulatory matters. She specializes in turning complex data and system behaviors into clear, regulator-ready findings, leading teams across de-anonymization analysis and app and website forensics. She earned her B.A. from the University of California Irvine and her M.S. from the University of California Berkeley.

Maddy Dwyer

Policy Analyst, Equity in Civic Technology, Center for Democracy and Technology (CDT)

Maddy Dwyer serves as a Policy Analyst on CDT's Equity in Civic Technology team, where she focuses on the responsible use of data and technology in the public sector, ensuring that privacy, transparency, and individual rights are centered. She particularly focuses on AI governance in state and local governments and public education.

Prior to joining CDT, Ms. Dwyer gathered extensive experience in public affairs and communications. She previously served as a Communications Associate with The Pew Charitable Trusts where she supported policy teams' strategic communications efforts, including building communications campaigns for their state and federal advocacy work and assisting with research publications. Before joining Pew, Ms. Dwyer was a

Communications Intern at CDT and has completed many communications and public affairs internships in industries such as cosmetics and personal care, healthcare, and water utilities.

Ms. Dwyer holds a Bachelor of Arts in American Studies from Stanford University, with a concentration in Race in American History and Politics, and a Master of Arts in Media and Strategic Communication from The School of Media and Public Affairs at George Washington University.

Dr. Nathan Good

Founder & CEO, Good Research

Dr. Nathan Good is a privacy and security expert and the Founder and CEO of Good Research. He works with organizations to assess and manage digital risk across apps, websites, AI systems, and data-sharing ecosystems. He helps leaders balance innovation with regulatory, reputational, and security risk through rigorous technical assurance and real-world testing. Dr. Good has advised Fortune 100 companies and government agencies and has testified before the U.S. House, Senate, and FTC.

David LeDuc

Vice President of Public Policy, Network Advertising Initiative (NAI)

David LeDuc is the Vice President of Public Policy, Network Advertising Initiative (NAI), the leading self-regulatory association for the third-party advertising industry. In this position, Mr. LeDuc works closely with member companies and represents the industry to promote a strong and responsible ad tech industry. Mr. Le Duc is a veteran of IT and public affairs, with extensive experience representing technology companies before the United States Congress, federal regulatory agencies, and state legislatures. Prior to joining NAI, Mr. LeDuc was the Senior Director for Public Policy at the Software & Information Industry Association, where he led the Association's technology policy efforts for more than 15 years across a wide range of IT issues such as data privacy and security, cybersecurity, digital platform responsibility, and open data standards. Mr. Le Duc is a graduate of West Virginia University with a degree in political science.

Richard Salgado

Principal Member, Salgado Strategies LLC

Richard Salgado teaches at Stanford and Harvard Law Schools. He also serves as an Advisory Board Member of American University Washington College of Law's Tech Law and Security Program, a Visiting Fellow on Security and Surveillance with the Cross-Border Data Forum, and a Senior Associate (Non-resident) with the Center for Strategic and International Studies. Mr. Salgado founded a consultancy to provide guidance to

organizations navigating cybersecurity and surveillance challenges. Mr. Salgado has over 35 years of experience across the private sector, government and academia, including as Google's Director of Law Enforcement & Information Security for 13 years, and as a prosecutor with the Computer Crime and Intellectual Property Section of the Justice Department.

Rebecca Kelly Slaughter

Commissioner, Federal Trade Commission

Rebecca Kelly Slaughter was sworn in as a Federal Trade Commissioner on May 2, 2018, and in 2024 she was unanimously confirmed by the Senate to serve a second term ending in 2029. In March of 2025, President Trump purported to fire her; the Supreme Court is currently considering her legal challenge to that removal in *Trump v. Slaughter*, argued in December 2025. To her FTC work, she brings extensive experience in competition, security, privacy, and consumer protection, and is known for building consensus around a progressive vision while advocating for the nation's consumers and workers.

Jacob Snow

Senior Staff Attorney, American Civil Liberties Union (ACLU) of Northern California

Jacob Snow is a Senior Staff Attorney at the ACLU of Northern California, where he works at the intersection of technology and civil rights. His policy and litigation advocacy work includes consumer privacy, government surveillance, automated decision systems, and the preservation of free speech online. At the ACLU, he has worked to bring attention to the harms of facial recognition on communities, brought litigation to protect the constitutional rights people targeted by the Trump administration on the basis of their speech, and represented tenants opposing AI-powered landlord surveillance in their homes. He has also advocated in the legislature and regulatory agencies for strong privacy rights and rights against automated systems. Before joining the ACLU of Northern California, Mr. Snow was a Staff Attorney in the San Francisco office of the Federal Trade Commission. He clerked for Judge Ronald M. Whyte in the Northern District of California and holds a J.D. from Georgetown Law.