

**Privacy in Peril:
When Unchecked
Commercial Surveillance and
Unbalanced Executive Power
Collide**

CPPA Presentation | Rebecca Kelly Slaughter

My Perspective

Background

- FTC Commissioner, 2018–?
- Acting Chair, FTC, 2021
- Chief Counsel, Senate Minority Leader Schumer
- Named plaintiff in Trump v. Slaughter (Supreme Court)

Core Thesis

- Unchecked commercial surveillance + unbalanced presidential power = qualitatively new privacy threat
- Mutually reinforcing problems, not simply parallel developments
- A President who controls agencies and who allies with dominant platforms can access comprehensive data on all Americans — without a warrant
- States and private enforcement are now the essential backstop

Commercial Surveillance

Where a notice-and-choice framework has landed us

FTC Commercial Surveillance Experience

Operative Protections

- FTC Act: prohibition on unfair and deceptive acts and practices
 - Unfairness three prong test:
 - 1) substantial injury
 - 2) Not reasonably avoidable
 - 3) Not offset by countervailing benefits to consumers or competition.
- COPPA: verified parental consent (plus underutilized provisions on minimization)
- Health Breach Notification Rule
- Safeguards Rule

Rulemaking Record

- Data Security and Commercial Surveillance rulemaking record - ongoing resource

Platform Cases

- Facebook/Meta (2011, 2019, 2023) (injunction/\$5B order violation/modification proceeding)
- Amazon (Alexa, Ring) (2023) (\$25 million penalty for COPPA violations; \$5.8 million for illegal video access)
- Google/YouTube (2019) (settlement for \$170 million civil penalty for COPPA violations)
- Many smaller cases as well

Smaller Companies ≠ Smaller Risk: FTC Case Examples

Gravy Analytics / Venntel

- 17 billion location signals/day from ~1 billion devices
- 1,000+ behavioral labels per consumer
- Tracked: religious attendance, reproductive health clinics, political events
- Sold to private companies AND federal agencies (DHS, DEA, FBI, IRS)

Mobilewalla

- Raw location data via real-time bidding
- No meaningful consent verification
- Tracked individuals at: military bases, DV shelters, union organizing events
- Built demographic profiles of racial justice protesters (2020)

Kochava

- "Staggering" amount of sensitive identifying info
- Precise geolocation + names, MAIDs, email, phone, income, ethnicity, political affiliation
- Court: selling 'encyclopedic information' plausibly causes substantial injury
- Court: privacy invasion itself = substantial injury

These are not edge cases — they are the logical products of a business model that incentivizes unlimited data collection.

Why Concentration — Not Just Collection — Is the Problem

Avoidance Becomes Impossible

In a healthy market, consumers can patronize rivals. When 2–3 firms control everything necessary for modern life, exit is not realistic. Kashmir Hill documented this: cutting Big Tech out of daily life is simply 'not possible.'

No Competitive Discipline

Dominant firms can engage in practices consumers would reject if they had meaningful choice, secure there is no adequate alternative. Privacy violations become economically rational.

Catastrophic Single Points of Failure

Diffuse data = contained breaches. Concentrated data = one accommodation exposes the entire population. Concentration converts data from a distributed risk into a systemic one.

Executive Power & Privacy

FTC, PCLOB, and the architecture of coercion

Why Independent Agencies Are Essential to Privacy

FTC — Commercial Surveillance

- Prevents unfair or deceptive acts in handling consumer data
- Enforces against the most politically connected tech companies
- For-cause removal protections ensure decisions are made on the merits, not politics
- A chilling effect on enforcement need not be explicit — the mere possibility of removal distorts institutional judgment
- Without independent commissioners, the public cannot know if powerful actors are escaping accountability via political favoritism

PCLOB — Government Surveillance

- Created post-9/11 to provide independent oversight of government surveillance programs (FISA, Section 702)
- Trump fired its Commissioners — removing the independent check on government surveillance
- Directly undermines EU adequacy commitments: EU adequacy depends on credible independent oversight of both commercial and government surveillance
- Without PCLOB, the U.S. cannot credibly commit to protecting the data of foreign nationals from government access

Executive Pressure on Private Actors

Bullying Law Firms & Universities

Executive orders revoked security clearances and terminated contracts for named law firms. Administration targeted 75+ universities, threatening to cut hundreds of millions in research grants to force changes to admissions, hiring, and campus speech policies.

Controlling Corporate Speech via FCC

Trump demanded monetary damages from ABC and CBS (each settling for \$16M). FCC Chair Carr threatened broadcast license revocations. Paramount canceled Stephen Colbert's show while seeking FCC merger approval for CBS. Local affiliates briefly pulled Jimmy Kimmel off air after FCC pressure.

FTC Used as Political Weapon

After minority commissioners were removed, the FTC issued a civil investigative demand to Media Matters — targeting a nonprofit that had published reporting critical of Elon Musk's X. A federal court found the CID was "a retaliatory act" and that Media Matters had engaged in "quintessential First Amendment activity."

Extracting Political Contributions

Trump's second inauguration drew 3× the previous record for million-dollar donors. Tech companies gave \$44.6M of \$245M total. Companies with federal business before the government — including Microsoft, Google, Amazon, and Palantir — donated over \$300M toward an unauthorized White House ballroom renovation.

The Architecture of Coercion

When These Converge

- President controls independent agencies
- Dominant platforms are political allies; understand their economic futures are caught up in relationship with the President.

Result

- Government-as-purchaser loophole: when regulators are politically controlled, buying commercial surveillance data becomes an executive permission slip.
- What they can't buy, they can coerce
- Ability to access detailed behavioral profiles of anyone in the country — location history, communications, health decisions, political associations — without a warrant, without judicial review, without oversight.

The Anthropic Example

From hypothetical to reality: the surveillance contract dispute

Anthropic sought explicit contractual protections prohibiting use of its AI for mass surveillance of Americans. DOD refused.

When Anthropic declined to accept DOD's terms, the administration terminated the contract and designated Anthropic a 'supply chain risk' — threatening to bar any government contractor from doing business with it.

OpenAI quickly stepped in.

The State Role

Data minimization · enforcement · private rights of action

Why States Are Now Essential — And What They Must Do

Data Minimization

- Prohibit collection beyond specific purpose
- Ban secondary uses and excess retention
- You can't strongarm data that doesn't exist
- FISA's minimization model for government should extend to commercial actors

State Enforcement of Commercial Practices

- Federal enforcement is now subject to political capture
- State AGs can pursue data brokers, surveillance advertisers, and platform abuses
- CPPA enforcement model: independent, expert, insulated from federal executive pressure
- Coordinate enforcement across state lines for national-scale actors

Private Rights of Action

- Enforcement cannot depend solely on agency discretion
- Agency discretion is now subject to political control
- Private enforcement creates distributed accountability that cannot be 'turned off' by replacing commissioners
- Essential backstop when federal watchdogs are dismantled

The Stakes

This is broader than privacy

When unchecked surveillance power and unbalanced market power converge, the result is a threat to democratic participation, civil liberty, and human dignity.