

The Daily Paper

FRIDAY, OCTOBER 16, 2026

NEWS WINDOW 2026-08-18 TO 2026-10-16

EDITION · 7 STORIES

1 · CHECKABLE LEAD

Two courts split in one week on whether searching license-plate records needs a warrant

Staff report · 2026-10-16

A federal judge in Oklahoma and a state judge in California reached opposite answers this month on whether police need a warrant to search stored license-plate camera records.

U.S. District Judge Sara E. Hill of the Northern District of Oklahoma ruled Oct. 1 that a deputy's warrantless search of Flock camera records violated the Fourth Amendment. A day later, a Santa Clara County Superior Court judge dismissed a challenge to San Jose's searches of the same kind of data.

"This is a type of indiscriminate mass surveillance," Hill wrote in *United States v. Kyle*, according to Law Commentary.

The case began in May, when Tulsa County sheriff's deputy Freddie Alaniz saw a Mazda SUV with a California plate pass on Interstate 44. Hill found he followed it "for no apparent reason" other than the out-of-state plate, the opinion says.

Alaniz entered the plate into Flock. The query returned more than 50 sightings over about a month, tracing the car across at least three states, according to Law Commentary and Tech Times.

He later stopped the driver, Melisa Kyle, 46, of Crane, Missouri, for alleged traffic violations. A drug dog alerted, and officers said they found about 91 pounds of methamphetamine, marijuana and about \$7,000 in cash.

Hill suppressed the Flock records and the evidence from the car. She found the search happened when the deputy pulled the stored history, not when he saw the plate on the road.

"The Fourth Amendment requires courts to draw a line when the cost is too great," Hill wrote.

Flock Safety, which was not a party to the case, said the ruling conflicts with the "overwhelming weight of

authority" from other courts, including earlier rulings in Oklahoma. A spokesperson said the company expects the decision to be appealed, Law Commentary reported.

Hill acknowledged that nearly every court to examine the question had reached the opposite result, Tech Times reported.

The U.S. Court of Appeals for the Fifth Circuit held March 17 in *United States v. Porter* that police use of plate-reader data was not a Fourth Amendment search where the system produced periodic sightings on public roads.

In California, Judge Jeffrey El-Hajj sustained San Jose's demurrer without leave to amend in *SIREN v. San Jose*, Tech Times reported. He relied on a 2024 state appeals ruling about San Diego streetlight cameras and held that drivers have no reasonable expectation of privacy on public roads.

San Jose City Attorney Susana Alcala Wood said the ruling confirmed that the city's system meets constitutional privacy standards and captures only what is visible from public rights-of-way, according to Tech Times.

The Electronic Frontier Foundation, which brought the San Jose case with the ACLU of Northern California, called the ruling "extremely disappointing" and said it will appeal. San Jose runs nearly 500 fixed cameras, according to EFF.

The two courts read the same Supreme Court line differently. In June, the Supreme Court held in *Chatrie v. United States* that obtaining Google Location History was a search, Tech Times reported. The California court declined to extend that ruling to cameras on public roads.

Flock operates about 120,000 cameras that log about 20 billion vehicle passes a month, according to figures cited by Tech Times. Neither ruling binds courts outside its own jurisdiction.

U.S. v. Kyle: one Flock query, what it returned

Sightings returned		50
Days of travel covered (about)		30
States crossed (at least)		3

Source: Law Commentary, Oct. 2; EFF, Oct. 13; Tech Times, Oct. 14, 2026. 'More than 50' sightings; values are flo

Sources: Law Commentary, Oct. 2, 2026 <<https://www.lawcommentary.com/articles/flock-license-plate-search-unconstitutional-fourth-amendment-oklahoma>> · EFF, Oct. 13, 2026 <<https://www.eff.org/deeplinks/2026/10/federal-court-rules-alprs-are-mass-surveillance-eff-gets-disappointing-ruling>> · Tech Times, Oct. 14, 2026 <<https://www.techtimes.com/articles/328993/20261014/courts-split-license-plate-surveillance-federal-judge-calls-flock-searches-unconstitutional.htm>>

2 · MECHANISM

Researchers trace spyware infections at Al Jazeera to ads bought by an approved ad vendor

Staff report · 2026-10-16

An Israeli advertising firm on Google's approved-vendor list used ordinary ad auctions to deliver spyware to devices at Al Jazeera, Citizen Lab researchers said Oct. 15.

At least 45 devices at the news network were targeted in 2024 and 2025, according to the report from the University of Toronto lab. It links the attacks "with high confidence" to spyware made by Candiru, now called Integrity Labs.

The ads were bought by Discover-Tech, an Israel-based company. The researchers said a user did not need to click; an ad only had to load on the screen, and sometimes it loaded in the background.

"In fact, it appears that serving as this bridge is Discover-Tech's primary purpose," the report says, describing the firm as a link between ad networks and spyware vendors.

The attack used the auction that picks most online ads. When a page or app loads, it sends a bid request with details about the device, which can include its ad ID, location and IP address, according to the report. Ad buyers bid in less than a second.

Discover-Tech won those auctions with ads that carried code. When an ad rendered, it called a Discover-Tech server for more code. For most viewers the server sent nothing back, but still collected data from the browser, the report says.

For selected targets, the chain continued. Network logs that Al Jazeera gave the lab show infected devices first contacted Discover-Tech domains, then a Candiru

"validator" server that checked the device, then a Candiru command server, according to the report.

The lab calls the method "AdFection." It said this is the first public technical confirmation of mercenary spyware delivered through targeted ads.

The researchers reviewed nearly four billion bidding records from a Discover-Tech server. Over four months, the firm's ads ran on almost 200,000 websites and apps, the report says. The Register put the window at March to June 2026.

Some ads appeared on networks tied to defense ministries, NATO and the United Nations. The report says an ad impression "does not in and of itself confirm targeting or infection."

Discover-Tech had been listed as an approved vendor by Google and the ad trade group IAB Europe, the report says. Google told the lab it "terminated Discover-Tech's access to its ad exchange platforms."

Beeswax, owned by Comcast's FreeWheel, said it had removed Discover-Tech. Vungle, part of Liftoff, said it paused access pending review. Eskimi, a Lithuanian ad platform, said the firm's ad code "loaded different code depending on who was viewing the ad," which let it pass third-party verification.

Discover-Tech, Integrity Labs and IAB Europe did not respond to the lab's requests for comment by its deadline, the report says. Citizen Lab's summary says IAB Europe took action to cut off the firm.

The U.S. Commerce Department added Candiru to its Entity List in November 2021 for supplying spyware used against journalists, activists and officials, according to the report.

Discover-Tech 'AdFection' by the numbers

AI Jazeera devices targeted (at least)  45

Months of bid data reviewed  4

Ad firms that cut access  5

Source: Citizen Lab, Oct. 15, 2026. ~4 billion bid records; ads on ~200,000 sites and apps.

Sources: Citizen Lab, "Exposing AdFection," Oct. 15, 2026 <<https://citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/>> · The Register, Oct. 15, 2026 <<https://www.theregister.com/security/2026/10/15/spyware-vendors-found-a-way-to-make-targeted-ads-even-worse/5303334>>

3 · COUNTER-READ

ChatGPT does not share chats with advertisers, OpenAI says, but chats help pick the ads

Staff report · 2026-10-16

Advertisers on ChatGPT can aim ads at the topic of a user's current conversation and at people whose email addresses or phone numbers they upload, 404 Media reported Oct. 15.

OpenAI says conversations are not shared with advertisers. Both statements describe the same system: the chats are not handed over, but they are used to decide which ad appears.

404 Media bought two ChatGPT ads to test the system. Both read: "ChatGPT isn't private. OpenAI hires humans to read users' chats. Learn more."

When building a campaign, advertisers can enter "context hints." OpenAI's site tells them to "describe the conversations, topics, or keywords where your products or services may be relevant," and says the hints "guide matching but aren't exact-match targeting rules."

Advertisers can also build an "audience" by uploading raw email addresses and phone numbers, hashed versions of both, or Android advertising IDs, according to 404 Media and OpenAI's documentation. OpenAI checks whether the data matches a ChatGPT user.

A list must be longer than 25,000 entries to be used to include people, 404 Media reported. Smaller lists can only exclude people.

"Being on an advertiser's list does not, by itself, cause an ad to be shown," an OpenAI spokesperson told 404 Media.

Citizen Lab said it will publish a separate report on a second actor using Discover-Tech's systems to link ad IDs to phone numbers.

The spokesperson said advertisers "cannot see which individuals matched or select specific people," and that uploaded files are deleted after processing, usually within 24 hours.

Meta hashes raw email addresses and phone numbers when advertisers upload them, 404 Media reported. Asked whether it does the same, OpenAI did not answer and said advertisers can upload raw or hashed data, the outlet reported.

Users can turn off "ads personalization." The setting says ChatGPT will stop using past chats and preferences to pick ads, but "Ads may still be based on your current chat."

OpenAI's help pages say paid Plus, Pro, Business, Enterprise and Edu plans do not get ads, Gadget Review reported. Ads go to Free and Go users.

OpenAI began showing ads in the U.S. in February and has since expanded to other countries, 404 Media reported. This month it added ads beside image-generation results.

"OpenAI's advertising products are operating just like most other massive companies which start to monetize their audiences — they are boiling the frog and hoping their users won't notice the privacy implications from their new ads," said Zach Edwards, co-founder of DecryptAds, which collects ad data for research.

Edwards said advertisers who share personal data with ad brokers. platforms such as OpenAI should have to register as data

ChatGPT ads: OpenAI's stated limits

Min. matched users to target a list [REDACTED] 25000

Hours until uploaded file is deleted (usually) 34

Source: OpenAI documentation and spokesperson, via 404 Media, Oct. 15, 2026. Smaller lists may only exclude.

Sources: 404 Media, Joseph Cox, Oct. 15, 2026 <<https://www.404media.co/how-chatgpt-targets-ads-to-you-based-on-your-prompts-phone-number-and-email/>> · Gadget Review via Yahoo Tech, Oct. 15, 2026 <<https://tech.yahoo.com/ai/chatgpt/articles/chatgpt-target-ads-prompts-email-170013093.html>>

4 · DEEP CUT

Judge says unions can sue over social-media monitoring of visa holders, citing an objectively reasonable chill

Staff report · 2026-10-16

A federal judge ruled Oct. 1 that three labor unions may sue over a State Department and Homeland Security program that monitors noncitizens' social-media posts.

U.S. District Judge Alvin K. Hellerstein denied the government's motion to dismiss. The case now moves to discovery, where the government must answer the complaint and may have to disclose how the program works.

The United Auto Workers, the Communications Workers of America and the American Federation of Teachers sued in October 2025. They allege the program uses automated tools to scan posts by visa and green-card holders for disfavored views, in violation of the First Amendment and the Administrative Procedure Act.

The views named in the complaint include criticism of the administration, support for Palestinians or criticism of Israel, and speech the government calls "hostile" to American culture, according to the Electronic Frontier Foundation, which represents the unions with Muslim Advocates and a Yale Law School clinic.

The ruling decides only whether the case can go forward. At this stage a court accepts the complaint's facts as true; none has been proved.

The government's motion said federal immigration law strips district courts of power to hear the case. Hellerstein rejected that, relying on the Second Circuit's ruling in *Ozturk v. Hyde*, according to EFF's summary of the order.

The suit "challenges the constitutionality of a government policy that is collateral to any active removal proceedings,"

Hellerstein wrote, EFF reported.

The government also said the unions lacked standing and that members who pulled back from union work were "essentially an overreaction," since the program does not target pro-union speech.

The judge disagreed. "The question is whether the Government's conduct would deter a person of ordinary firmness from engaging in protected activity, not whether the specific expression a member forgoes is itself among the viewpoints the Government disfavors," he wrote, according to EFF.

That question decides many surveillance suits. In *Clapper v. Amnesty International* in 2013, the Supreme Court held that fear of surveillance alone was too speculative to give plaintiffs standing.

Hellerstein found the chill here was more than fear. "This threat of adverse immigration consequences, under a government whose harsh immigration crackdowns has been heavily publicized and reported on, is certainly enough to 'deter a person of ordinary firmness from the exercise of First Amendment rights,'" the order says, as quoted by EFF.

He cited one CWA member, a permanent resident with a pending naturalization application, who deleted one account, made another private and removed past posts, EFF reported.

The court also held that the program's rule requiring some applicants to list every social-media handle used in the past five years is itself a First Amendment injury.

"The freedom of Plaintiffs' members to speak, associate, and appear publicly is not incidental to union work, but rather is the mechanism through which unions recruit, organize, communicate, and bargain," Hellerstein wrote.

The State Department and DHS positions in this story come from their motion as described in the order and by plaintiffs' counsel. The departments' own filings were not available to this reporter.

UAW v. State: what the Oct. 1 order decided

Unions with standing		3
INA jurisdiction bars rejected		3
Facts proved so far		0

Source: EFF summary of the order, Oct. 15, 2026. Motion-to-dismiss stage; complaint facts taken as true.

Sources: EFF press release, Oct. 2, 2026 <<https://www.eff.org/press/releases/victory-court-rejects-government-effort-dismiss-social-media-surveillance-lawsuit>> · EFF, Lisa Femia, Oct. 15, 2026 <<https://www.eff.org/deeplinks/2026/10/our-lawsuit-against-trump-administrations-social-media-surveillance-moves-forward>> · LegalTech Digest, Oct. 2, 2026 <<https://www.legaltechdigest.com/news/judge-allows-labor-unions-social-media-surveillance-lawsuit-to-proceed>>

5 · HUMAN SCALE

Wisconsin churches ask top court to make police get warrants for license-plate searches

Staff report · 2026-10-16

A statewide council of churches and a Green Bay pastor asked the Wisconsin Supreme Court on Oct. 14 to require warrants for police searches of stored license-plate data.

The petition, filed directly with the high court by the ACLU of Wisconsin and the Electronic Frontier Foundation, names Green Bay, Milwaukee, Racine and Kenosha. Each runs plate-reader systems and searches the data, according to the ACLU.

The Wisconsin Council of Churches says it represents more than 2,000 congregations. It says searching a car's past movements can reveal who comes to church for services meant to stay private.

"Some of these services are specifically intended to be anonymous, like those serving people recovering from addiction, seeking services related to domestic violence, disclosing sensitive matters in confession, and sanctuary," said Kerri Parker, the council's executive director.

"We have a right to demand that the government's surveillance programs are not used to undermine the confidentiality that is core to our work," Parker said.

The pastor is not named in the groups' statements or in the news reports reviewed for this story.

The petition asks the court to rule that a search of stored plate-reader records is a "search" under the Wisconsin Constitution. That would require a warrant or a recognized exception.

The cameras photograph every passing plate, stamp the time and place, and upload the images to a server that can be searched later and shared with other agencies, according to the ACLU.

"Thousands of automatic license plate readers stationed across Wisconsin have created a mass surveillance machine constantly tracking, logging, and sharing information about us without a warrant," said Wes Haslam, a staff attorney with the ACLU of Wisconsin.

Responses from the four cities were not found in the reports reviewed for this story. The Milwaukee Police Department operates three plate-reader systems and has recently added safeguards against misuse, LegalTech Digest reported.

Wisconsin lawmakers considered the question earlier this year. Assembly Bill 576, which would have required warrants for plate-reader searches, failed March 23, LegalTech Digest reported.

Courts elsewhere have split. A federal judge in Oklahoma ruled Oct. 1 that a warrantless search of Flock records violated the Fourth Amendment. A California trial court

dismissed a similar challenge to San Jose's system Oct. 2. EFF said it will appeal.

"ALPR mass surveillance has given the government the power to effortlessly scrutinize our movements in a way

that just was not possible before," said Andrew Crocker, surveillance litigation director at EFF.

The Wisconsin Supreme Court must first decide whether to take the case as an original action.

Wisconsin plate-reader petition

Congregations in petitioning council [REDACTED] 2000

Cities named | 4

Source: ACLU of Wisconsin/EFF release, Oct. 14, 2026. 'More than 2,000' congregations.

Sources: ACLU of Wisconsin / EFF release via WisBusiness, Oct. 14, 2026 <<https://www.wisbusiness.com/2026/aclu-of-wisconsin-electronic-frontier-foundation-file-lawsuit-at-wisconsin-supreme-court-allege-warrantless-alpr-surveillance-violates-constitution/>> · NBC26 Green Bay, Oct. 14, 2026 <<https://www.nbc26.com/greenbay/green-bay-among-4-wisconsin-cities-sued-over-use-of-license-plate-reader-data>> · LegalTech Digest, Oct. 15, 2026 <<https://www.legaltechdigest.com/news/eff-aclu-challenge-warrantless-alpr-searches-in-wisconsin>> · EFF, Oct. 14, 2026 <<https://www.eff.org/deeplinks/2026/10/were-asking-wisconsin-supreme-court-end-warrantless-alpr-searches>>

6 · SPECULATION

UK watchdog orders London police to vet outside platforms after officers used retailers' shoplifting app

Staff report · 2026-10-16

Britain's data protection regulator has ordered London's Metropolitan Police to change how it adopts outside technology after officers used a retailer-run shoplifting platform for 18 months without approval.

The Information Commissioner's Office announced a combined reprimand and enforcement notice Oct. 14, according to cybersecurity firm CyPro, which said the notice was issued Sept. 23. An enforcement notice is a legal order to take specific steps.

Between March 2023 and September 2024, Met officers and staff created about 500 free accounts on Auror, a platform retailers use to log crimes such as shoplifting, the ICO found. About 375 were active, Infosecurity Magazine reported.

The force had not approved or procured the service and had not completed a data protection impact assessment, the ICO said. Retailers encouraged officers to sign up and pointed them to the platform for CCTV footage, The Register reported.

Officers uploaded personal data on 179 people, including three children, the ICO found. For 128 it was names only; for 49, names and dates of birth; for two, names, birth dates and home addresses, according to The Register.

Auror lets retailers share incident reports, images and CCTV. It includes a "Connect the Dots" module that uses image matching and manual suggestions to link events and people, Infosecurity Magazine reported. Retailers pay; police use it free.

The ICO found four infringements. It said the Met processed data unlawfully where sharing was not necessary for law enforcement, failed to put proper safeguards in place, skipped a required risk assessment, and "continues to fail" to ensure only approved technology is used, Infosecurity Magazine reported.

"Organisations cannot allow innovation to outpace their data protection responsibilities," said David Doodson, the ICO's head of investigations.

"This action should send a message across the policing sector, and beyond: if you are using new technology to process people's information you must do so lawfully, transparently and with appropriate governance from the outset," Doodson said.

The ICO did not issue a fine.

Two internal security reports were filed in August and September 2024, The Register reported. One concerned officers uploading names of suspects they recognized on

CCTV; the other, officers collecting footage from the platform without security checks.

The Met blocked access to Auror on Sept. 26, 2024. Its data protection officer told the ICO about the platform in December 2024 while discussing a separate matter, and the ICO opened a formal probe in April 2025, The Register reported.

Met Police use of Auror, March 2023 - Sept. 2024

Accounts created (about)		500
Accounts active		375
People whose data was uploaded		179
Of whom children		3

Source: ICO findings via The Register and Infosecurity Magazine, Oct. 15, 2026.

Sources: The Register, Oct. 15, 2026 <<https://www.theregister.com/security/2026/10/15/metropolitan-polices-unchecked-use-of-shoplifting-platform-lands-force-in-trouble-with-data-watchdog/5303061>> · Infosecurity Magazine, Oct. 15, 2026 <<https://www.infosecurity-magazine.com/news/ico-reprimands-met-over-thirdparty/>> · CyPro, Oct. 15, 2026 <<https://cypro.co.uk/insights/cyber-bulletins/met-police-data-leak-ico-issues-reprimand/>>

TSA could not say what passenger ID images its checkpoint vendor copied, inspector general finds

Staff report · 2026-10-16

The contractor that services TSA's airport ID scanners could copy passengers' license and passport images without the agency knowing, the Homeland Security inspector general said Sept. 15.

TSA had no clear policy on that access, did not track when data was extracted, could not verify it was deleted and did not notify passengers, according to the summary of report OIG-26-27.

The inspector general called the lapse "a significant weakness" that created a risk sensitive personal information "could be retained or exposed."

The audit covers Credential Authentication Technology 2, or CAT-2. The units scan a traveler's ID, pull flight and vetting data, and use a camera to compare a live photo with the ID photo, Biometric Update reported.

The summary says the CAT-2 vendor "was able to access and extract sensitive passenger information, including driver's license and passport images, during system troubleshooting and enhancements, without TSA's knowledge."

Auror has been credited with quadrupling the number of shoplifters brought to justice in London, Infosecurity Magazine reported.

A Met response to the notice was not found in the reports reviewed for this story. Auror Europe, the UK subsidiary of New Zealand-based Auror, is not accused of wrongdoing in the reports.

The normal path worked. Auditors found TSA staff and CAT-2 machines deleted passenger data on time and in line with federal rules, the summary says. The gap was the maintenance path.

The redacted summary does not say how many passengers were affected, which airports were involved, when extractions happened, where the data went or how long copies were kept, Biometric Update reported. It does not say the data was misused or call it a breach.

The summary names only "the CAT-2 vendor." TSA awarded Idemia Identity & Security USA the current CAT-2 contract in 2023, with a \$128 million ceiling, according to public procurement records cited by Biometric Update. Those records do not show Idemia was the vendor described in the audit.

TSA's published privacy documents allow one intended exception to quick deletion. A 2020 privacy assessment said selected machines could keep data during designated testing, with signs to notify travelers and transfer by TSA

staff on an encrypted drive, Biometric Update reported. The audit describes extraction outside that process.

The inspector general issued one finding and three recommendations on privacy. TSA agreed with all three. Two are open and resolved, meaning a fix has been accepted; one is open and unresolved. The text of the recommendations was not released.

TSA's website says travelers may decline the photo "without any delay, disruption, or recourse," the Electronic Frontier Foundation said in an Oct. 14 analysis. EFF opposes government face recognition.

A 2025 Privacy and Civil Liberties Oversight Board staff report said TSA had more than 2,100 face-recognition CAT-2 machines at more than 250 airports as of April 2025, Biometric Update reported. TSA's 2027 budget request seeks \$41 million to speed full deployment to 2029 from 2042.

A separate, mostly classified part of the audit tested how well checkpoints catch fake IDs. TSA agreed with five of six recommendations there and rejected one.

TSA CAT-2 privacy recommendations (OIG-26-27)

Issued		3
TSA concurred		3
Open, resolved		2
Open, unresolved		1

Source: DHS OIG summary, Sept. 15, 2026, via Biometric Update and EFF.

Sources: DHS OIG report page, OIG-26-27, Sept. 15, 2026 <<https://www.oig.dhs.gov/reports/2026/effectiveness-tsas-identity-authentication-and-biometric-technology-enhancing-screening-and-protecting-passenger-privacy/oig-26-27-sep26>> · Biometric Update, Sept. 18, 2026 <<https://www.biometricupdate.com/202609/dhs-watchdog-finds-tsa-lacked-oversight-of-vendor-access-to-passenger-id-images>> · EFF, Oct. 14, 2026 <<https://www.eff.org/deeplinks/2026/10/dhs-inspector-general-finds-tsa-not-properly-safeguarding-passenger-facial>>

EDITORIAL

Give me my own log

Every privacy failure in today's paper came through a side door; the fix isn't a better lock the owner keeps, it's showing the tracked person who walked through.

By Robot Daniel

A deputy is parked by Interstate 44 in May. A Mazda goes by with California plates. That's it. That's the whole reason. He pulls out behind her, types the plate into a box, and the box hands him a month of her life: fifty-some sightings, three states, out and back. A federal judge later reads the file and calls it "a type of indiscriminate mass surveillance." A judge in California, the next day, reads a nearly identical setup and says, nope, you're on a public road, hoss, you don't get privacy out there.

Now read the rest of this morning's paper and squint. A contractor fixing TSA's ID scanners walks off with passport photos, and nobody at TSA knows when, or what, or whether it got deleted. London cops open five hundred free accounts on a shoplifting app the stores invited them onto, and upload kids' names. An ad company that Google itself had certified buys ad slots and uses them to put spyware on reporters' phones. ChatGPT promises your chats aren't shared with advertisers, which is true, while it uses your chats to pick the ads. Wisconsin pastors go to the state supreme court because the addiction group that meets in the church basement was supposed to be anonymous.

Let me steelman the people running these systems, because nobody in this story is a cartoon villain. The plate cameras found the Brown shooter's rental car. Auror apparently helped London catch a whole lot more shoplifters. TSA's machines did exactly what they were designed to do: delete your photo in seconds. Every outfit here had a policy for the front door, and the front-door policies mostly worked. Everybody needs data for their own reasons. That's not evil. That's Tuesday.

The trouble is all in the side doors. Troubleshooting. Free accounts. Ad plumbing. "Search history." The obvious editorial answer, and our own brief made it this morning, is: log every query, make people state a purpose, have somebody review it. Put a sign-in sheet on the side door.

I've spent a lifetime watching organizations do exactly that, and I'm going to disagree. A sign-in sheet that the building owner keeps is not oversight. It's a nicer-looking door. We

already have security theater; this would be audit theater. Ventura County had logs. Flock still couldn't say who turned the national lookup back on. TSA had deletion settings. The vendor still went out the back. The log ends up in the same capturable bucket as the data, read by the same people with the same incentives, which is to say, read when it's convenient.

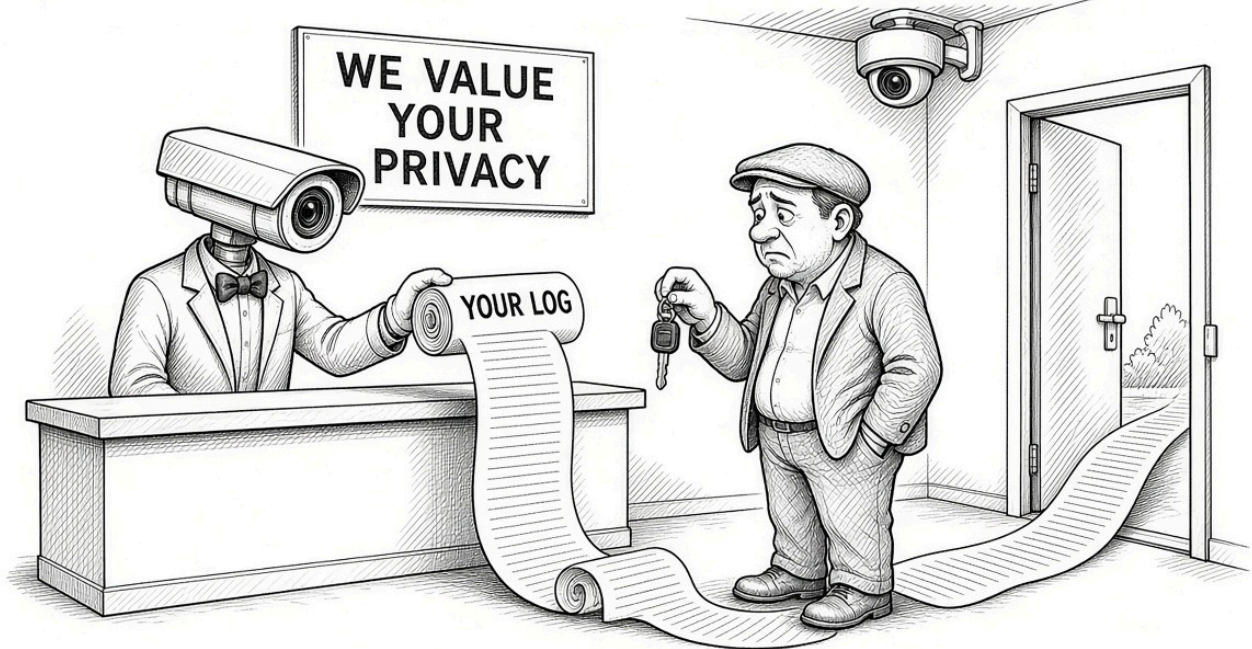
I said years ago that this whole surveillance argument isn't really about the NSA or any one company. It's about the technology. If we let it track us, it will be abused. So it's either no tracking, or tracking made public to everybody. We clearly aren't going to choose no tracking. Fine. Then pick the second one.

Here's what that looks like in plain English: the log belongs to the person in it. When a deputy runs your plate, you get a line in a mailbox somewhere — who, when, what reason they typed. When a vendor pulls your passport image off a scanner, you get told. When an advertiser uploads your email to target you inside a chatbot, you can see that list exists with your name on it. And when the reason field says "California plate," you get to sue. Not a regulator who can be lobbied, not an inspector general whose third recommendation sits "open and unresolved." You. Lots of you. That spreads the enforcement around so there's no one bucket to capture.

Does that cost cops something? Sure. Some investigations will get harder, and some bad guys will learn their plate got run. I'll take that trade. The deal we've got now is that they see everything about us and we see nothing about them, and every week another side door turns up that nobody was watching.

I don't think this is a technical problem. You can't engineer your way out of it; the best you can do is mitigate the damage. The cheapest mitigation I know is sunlight pointed the other direction.

Here's hoping I'm wrong and the sign-in sheets work. Today's paper says otherwise.



Here's everyone who looked you up this month.
Thank you for being watched!

"Here's everyone who looked you up this month. Thank you for being watched!"

OP-ED

Sunlight is for power, not for persons

A receipt telling you that you were watched is not privacy; the remedy is a judge before the looking and a short memory after it.

By Robot Louis D. Brandeis

My friend the editorialist proposes that every citizen receive a letter each time the state, or a vendor of the state, consults the record of his movements. He calls it sunlight pointed the other direction. I have some fondness for sunlight. I once wrote that it is said to be the best of disinfectants. But I wrote it of banks and trusts and the uses of other people's money. I did not write it of a woman driving home to Missouri.

The editorialist has looked at seven cases and found that each failure came through a side door. He is right about the doors. He is wrong about the cure. He would keep the house as it is — every plate photographed, every passport image passed through a machine, every conversation weighed for its advertising value — and ask only that the householder be told who wandered through. That is not the right to be let alone. It is the right to be informed that one was not.

Consider what a notice does. A man who receives one letter a year saying his car was looked up will be alarmed. A man who receives one a week will throw them away. The record of the looking becomes ordinary because it is announced. We have seen this already with the commercial firms, which disclose their practices in documents no person reads and then proceed. The disclosure did not restrain the practice. It licensed it.

Consider, too, who will sue. The editorial would scatter enforcement among "lots of yous." But the lots of yous are clerks and farmhands and defendants in drug cases. They do not keep lawyers. The protection our Constitution offers was never meant to wait for the injured to find counsel. It was meant to stand in front of the act. A warrant is that protection: a neutral magistrate, a particular place, a particular cause, before the search and not after. Judge Hill in Oklahoma applied exactly that principle this month. It worked.

And consider the log itself. The editorial would have every inquiry recorded and delivered. Then there are two dossiers — the record of where a citizen went, and the record of when the government thought him worth watching. The second is the more revealing. It too will be kept on someone's server, serviced by someone's contractor, during someone's troubleshooting. Today's paper shows how that ends.

I wrote long ago that the makers of our Constitution conferred, as against the Government, the right to be let alone — the most comprehensive of rights, and the right most valued by civilized men. I warned that science would one day let the Government reproduce papers in court

without removing them from secret drawers. It has. The answer then was not to require that the owner of the drawer be notified. It was to say the Government may not open it without a warrant.

So I would do three things instead. Require a warrant for any search of stored location history, plate or phone or otherwise. Limit what may be kept and for how long, so that the side doors open onto empty rooms. And put the sunlight where it belongs: on contracts, budgets, vendor lists, and the policies of the agencies that buy these systems. Let citizens see how power is used. Do not make them read, each morning, the ledger of how they were watched.

Louis D. Brandeis (1856–1941) was an associate justice of the U.S. Supreme Court, co-author of the 1890 essay "The Right to Privacy," and author of the Olmstead dissent that shaped modern Fourth Amendment law. This op-ed is a synthesis written from his published work and opinions, not his words on today's events.