



Written by [Veronika Kyrylenko](#) on March 20, 2026

Patel Confirms FBI Buying Americans' Location Data

FBI Director Kash Patel confirmed that the bureau is buying commercially available data that can track people's movements and reconstruct their location history. The practice sits at the center of a growing legal and constitutional dispute.

Patel told Senators during the Intelligence Committee's annual Worldwide Threats [hearing](#) on Wednesday:

We do purchase commercially available information that's consistent with the Constitution and the laws under the Electronic Communications Privacy Act, and it has led to some valuable intelligence for us.



AP Images
Kash Patel

The admission is direct. Federal law enforcement is using a pathway that sidesteps one of the core safeguards of the American system: the warrant requirement.

The FBI Practice

The FBI's position marks a clear shift from its stance of just a few years ago. In 2023, then-Director Christopher Wray [told lawmakers](#) the bureau was no longer purchasing location data derived from commercial sources. He acknowledged that such data had been acquired in the past for "a specific national security pilot project," but said the effort was no longer active.

That position no longer holds.

During the Wednesday hearing, Senator Ron Wyden (D-Ore.) revisited Wray's statement and pressed Patel on whether the FBI had resumed the practice and whether he would commit to stopping it.

Patel answered by confirming that the bureau relies on commercially available data as part of its investigative toolkit "to do our mission."

Wyden then warned that acquiring Americans' location data without a warrant amounts to "an outrageous end-run around the Fourth Amendment." He cautioned that the risks are amplified as artificial intelligence enables rapid analysis of vast volumes of personal data.

The exchange made one point clear: What had been described as a past, limited effort is now an active and defended practice.

ECPA

Patel's defense rests in part on compliance with the [Electronic Communications Privacy Act](#), or ECPA. Enacted in 1986, the law governs how electronic communications are accessed and disclosed by the government and service providers.

But ECPA was built for a very different technological era. It predates smartphones, app ecosystems,



Written by [Veronika Kyrylenko](#) on March 20, 2026

cloud computing, and the modern data brokerage industry. At its core, the statute draws a legal distinction between the content of communications and non-content data, often referred to as metadata. Content, such as a phone call or the body of an email, generally requires a warrant. Metadata, such as routing information or transactional records, has historically been subject to lower legal thresholds.

That distinction has become increasingly strained. As the Supreme Court recognized in *Carpenter v. United States*, certain forms of metadata, particularly location data, can be deeply revealing (more on that later), and are protected by Fourth Amendment.

ECPA also has been expanded and modified over time. Congress amended the framework through laws such as the Communications Assistance for Law Enforcement Act of 1994, the USA PATRIOT Act of 2001 and its reauthorizations, and the FISA Amendments Act of 2008. These changes broadened unconstitutional surveillance authorities in various contexts.

As surveillance powers expanded, the constitutional limits governing them were left for the courts to define.

The Fourth Amendment in the Digital Age

In 2018, the Supreme Court came up with a clear rule: If law enforcement wants your location data from your phone carrier, it needs a warrant. That standard comes from the decision in [Carpenter v. United States](#).

Before that ruling, courts often relied on the “third-party doctrine,” the idea that information shared with a company carries reduced privacy protections. The Court rejected that logic for location data. It emphasized that privacy does not disappear simply because a person moves through public space. “A person does not surrender all Fourth Amendment protection by venturing into the public sphere,” the Court wrote, adding that what one seeks to keep private may still be constitutionally protected.

The justices focused on how sensitive location data has become:

Mapping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his “familial, political, professional, religious, and sexual associations.”

Because of that sensitivity, the Court held that obtaining historical cell-site location information is a Fourth Amendment search. As a result, “the Government must generally obtain a warrant supported by probable cause” before acquiring it.

The warning was explicit. Without limits, the government could track a person “every moment of every day,” creating what the Court described as “tireless and absolute surveillance.”

But the ruling had a clear boundary. It applied to records held by telecom providers. It did not address what happens when similar data is collected, aggregated, and sold in the private marketplace. That gap, now known as the data broker loophole, sits at the center of the current debate.

Closing the Data Broker Loophole

Lawmakers from both parties are now moving to close the data broker loophole. On March 12, Representatives Zoe Lofgren (D-Calif.) and Warren Davidson (R-Ohio), along with Senators Wyden and



Written by [Veronika Kyrylenko](#) on March 20, 2026

Mike Lee (R-Utah), [introduced](#) an updated version of the Government Surveillance Reform Act.

The bill directly targets the use of commercially available data as a workaround to constitutional limits. It would require federal agencies to obtain a warrant before purchasing Americans' personal data, effectively placing brokered information under the same legal standard as records held by telecom providers. The provision is a part of a broader reform of Section 702 of the Foreign Intelligence Surveillance Act (FISA) "and other government surveillance programs," said the legislators.

Representative Davidson said the bill would close "the data broker loophole that allows the federal government to spy on citizens by purchasing private data that would otherwise require a warrant or subpoena."

Wyden framed the issue as a mismatch between law and technology:

Advances in technology, from AI to the explosion of Americans' data available for purchase, have far outpaced the laws protecting Americans' privacy and civil liberties.

The reform, he argued, would allow the government to combine security objectives with liberty protection, which, he said, "are not mutually exclusive."

Supporters say the bill is not about limiting legitimate investigations. It is about restoring a basic principle. If the government needs a warrant to obtain sensitive data directly, it should not be able to bypass that requirement simply by buying it.

When Surveillance Is for Sale

Not everyone agrees that reform is necessary. Intelligence Committee Chair Senator Tom Cotton (R-Ark.) defended the practice.

"The key words are commercially available," he said during the hearing. He continued,

If any other person can buy it and the FBI can buy it and it helps them locate a depraved child molester or savage cartel leader, I certainly hope the FBI is doing anything they can to keep Americans safe. It's not much different from long-standing Supreme Court precedent that, for instance, says law enforcement can go through trash that you put on the side of the curb because you no longer have a privacy interest in it.

The logic is simple, but flawed.

First and foremost, it treats availability as a substitute for constitutionality. The Fourth Amendment does not hinge on whether data is for sale. It limits what the government can access without judicial approval.

The analogy to abandoned trash also fails. Trash is discrete and voluntary. Location data is continuous, passively collected, and far more revealing. As the Supreme Court recognized in *Carpenter*, it can reconstruct a person's life.

Finally, the argument relies on extreme cases to justify broad authority. The same power used to pursue serious criminals applies to everyone, without a warrant.



Written by [Veronika Kyrylenko](#) on March 20, 2026

Big Brother Is Watching You

The risk grows as federal systems move toward deeper integration of personal data.

Last May, the Trump administration [contracted with Palantir](#) to merge datasets across agencies, from tax records to health data and other sensitive government-held information, raising the prospect of a unified profile of everyday Americans. At the same time, the administration has started enforcing [REAL ID](#) requirements while [advancing](#) unconstitutional federal voter ID measures, expanding the scope of centralized identity systems.

In that environment, commercially purchased data does not sit in isolation. It feeds into a broader surveillance architecture, one that becomes more powerful as more pieces are connected.

Related:

[FISA Section 702 Nears Expiration As Congress Considers Warrant Requirements](#)



Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.