Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

# Artificial Intelligence and the Fourth Amendment: Two Emerging Legal Issues

May 5, 2026

Various law enforcement components at the federal, state, and local levels report using artificial intelligence (AI) for some functions. Legislatures at the state and federal level have considered a variety of proposals relevant to the intersection of law enforcement, crime, and AI. Legal commentary has focused on the potential impact of AI on criminal justice, including everything from the admissibility of AI evidence, to sentencing, to AI-powered robot police officers, to the Fourth Amendment.

Precise conceptualizations of AI vary, but the FBI has used the definition from the 2019 National Defense Authorization Act. That legislation defines AI to include, among other things, artificial systems "designed to think or act like a human," or that "perform[] tasks under varying and unpredictable circumstances without significant human oversight," or that "can learn from experience and improve performance when exposed to data sets." Another federal statute defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments" and that uses human or machine inputs to perceive environments, abstract its perceptions, and thereby "formulate options for information or action."

This Legal Sidebar focuses on the potential Fourth Amendment implications of AI in two contexts. The first pertains to law enforcement seeking to obtain data generated from consumer use of AI products such as chatbot conversation histories and related data. The second context involves law enforcement use of surveillance tools augmented with AI, with a particular focus on Automated License Plate Readers (ALPRs). This Legal Sidebar begins with a brief overview of Fourth Amendment concepts relevant to both topics and concludes with considerations for Congress. For a list of additional CRS products covering other aspects of AI, *see* CRS Insight IN12458, *Artificial Intelligence: CRS Products*, by Laurie Harris and Rachael D. Roan (2025).

## The Fourth Amendment and AI

The Fourth Amendment imposes limits on searches and seizures by the government. Courts have determined that a Fourth Amendment search occurs if "the Government obtains information by physically intruding on a constitutionally protected area" or "when the government violates a subjective expectation of privacy that society recognizes as reasonable." With respect to the seizure of property, that "occurs

**Congressional Research Service**
https://crsreports.congress.gov
LSB11429

when there is some meaningful interference with an individual's possessory interests in that property." If a law enforcement activity qualifies as a search or seizure, then the Fourth Amendment requires that it must be reasonable, which ordinarily means that the search or seizure must be conducted pursuant to a warrant supported by probable cause, with some exceptions.

## Law Enforcement Access to Chatbot User Data

Consumer use of AI products generates data that may be of interest to law enforcement in criminal investigations. For example, investigators have sought or used chatbot conversation histories as evidence in cases involving a range of offenses, including arson, child exploitation, fraud, and vandalism. In an arson prosecution stemming from the Lachman Fire and the Palisades Fire, for instance, the government alleged in charging documents that the defendant had various exchanges with OpenAI's ChatGPT, a generative AI program, on the topic of fire, including asking the program: "Are you at fault if a fire is [lit] because of your cigarettes."

In some cases, it appears that law enforcement has obtained chatbot user data by accessing a suspect's phone or device. To illustrate, in one vandalism case, local law enforcement seized a suspect's phone as evidence. According to law enforcement, the suspect provided a passcode and consent to search the device. Law enforcement obtained incriminating ChatGPT conversations where the suspect asked ChatGPT about the consequences of smashing windshields and otherwise damaging vehicles. (Federal courts have expounded on the various, potential legal considerations when law enforcement accesses a suspect's device—topics beyond the scope of this product.)

In other cases, however, it appears that law enforcement has sought chatbot user data from AI companies. In such scenarios, the extent to which users' data such as chat histories are protected by the Fourth Amendment may hinge in large part on the limits of the third-party doctrine, which the Supreme Court has held to mean that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." The third-party doctrine reflects a judgment that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." In articulating this doctrine, the Supreme Court in 1976 concluded that a bank customer lacked a reasonable expectation of privacy in financial records stored with his bank by virtue of his being a customer there. Under a broad construction of the third-party doctrine in the modern era, a potentially vast amount of digital information would exist beyond the protections of the Fourth Amendment, because such information is often shared by customers with technology providers in the ordinary course of using a product.

In the 2018 opinion *Carpenter v. United States*, the Supreme Court recognized a limitation to the potentially expansive scope of the third-party doctrine. That case involved the warrantless search of historical cell-site location information (CSLI)—data that record the location of a cellular device when it connects to "a set of radio antennas called 'cell sites'" typically mounted on towers or structures and operated by private companies to provide network coverage. In *Carpenter*, law enforcement obtained a defendant's CSLI—covering 127 days—from cellular providers through a court order issued pursuant to the Stored Communications Act (SCA). The *Carpenter* Court held that the CSLI was not exempt from Fourth Amendment protection pursuant to the third-party doctrine, even though the CSLI was shared by the defendant with cellular providers in the course of his cell phone use. The Court rejected the idea that the defendant's sharing of CSLI with the providers was voluntary, observing that "[c]ell phone location information is not truly 'shared' as one normally understands the term" given that carrying a cell phone is "indispensable to participation in modern society" and in light of the fact that "a cell phone logs a cell-site record by dint of its operation." In addition, the Court concluded that the defendant had a reasonable expectation of privacy in the CSLI due to the revealing nature of the information at issue. This, the Court observed, amounted to "near perfect surveillance" because cell phones accompany their owners in nearly every physical space and because the CSLI is both accurate and retrospective. As the Court in *Carpenter*

put it, CSLI can provide "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.'" Nevertheless, the Court described *Carpenter* as a "narrow" holding that did not abolish the third-party doctrine or predetermine its application to other forms of technological surveillance.

It appears that federal courts have not yet had the occasion to determine whether a user maintains a reasonable expectation of privacy in chatbot histories, or whether that expectation is forfeited by virtue of the third-party doctrine. A Supreme Court case argued in April 2026—discussed below—may shed additional light on the scope of *Carpenter* and on the types of technologies that are protected by the Fourth Amendment by virtue of their indispensability in modern society and the revealing nature of the data they generate. In practice, it appears that law enforcement may already be seeking warrants for some such information pursuant to a statutory scheme—namely, the SCA.

### The Stored Communications Act and Chatbot Data

Law enforcement access to chatbot user data implicates the Stored Communications Act (SCA). Congress enacted the SCA as part of the Electronic Communications Privacy Act (ECPA). Some legislative history suggests that Congress's intent in doing so was to add supplemental protections from providers' disclosure of stored wire and electronic communications beyond those potentially covered by the Fourth Amendment. For instance, the Senate Judiciary report accompanying the ECPA described the proliferation of electronic data storage and the risk that such data "may be subject to no constitutional privacy protection" because it "is subject to control by a third party computer operator." In general terms, the SCA restricts when certain information may be disclosed by Electronic Communication Services or Remote Computing Services, which typically include entities such as "cell phone providers, email providers, or social media platforms" and cloud computing providers. Pursuant to a provision of the SCA codified at 18 U.S.C. § 2703, the government may compel such providers to share communications' content and metadata if it obtains the requisite level of legal process, which ranges from a subpoena to a warrant, depending on the category of information sought. Analysis of the SCA and related considerations may be found in CRS Legal Sidebar LSB10801, *Overview of Governmental Action Under the Stored Communications Act (SCA)*, by Jimmy Balser (2022).

## Reverse Warrants for Chatbot Histories

*Carpenter* involved a law enforcement search for customer data pertaining to a *known* suspect. In other words, law enforcement had already identified the defendant as a possible suspect when it obtained a court order compelling certain wireless carriers to provide that person's phone records. In the digital space, law enforcement sometimes works in the opposite direction—seeking customer data to identify an *unknown* suspect. Take, for example, a suspected arson where law enforcement knows the time and address of the fire, but has not been able to identify a suspect through traditional investigative means. There, law enforcement might seek a reverse keyword warrant to compel a technology provider to disclose account information for users who searched for the address of the suspected arson in the fifteen days preceding the fire. Similarly, if investigators know the time and location of a robbery, but lack other leads, they might request a geofence warrant to compel a technology provider to disclose information about smartphone users who were near the robbery scene around the time it occurred.

Reverse warrants, like geofence and reverse keyword warrants, seek to identify a suspect by compelling technology providers to identify user accounts that match the criteria specified in the warrant. Some legal observers have argued that chatbot user data may provide another pool of user data from which law enforcement might seek to identify suspects in this manner. It appears that at least one reverse chatbot warrant may have already been obtained at the federal level. In September 2025, federal authorities obtained a warrant for chatbot user data in connection with a child exploitation investigation. According to the warrant affidavit, investigators had been unable to identify the suspect beyond an online username. The suspect had, however, told an undercover investigator online about several exchanges the suspect had with ChatGPT, unrelated to the crime being investigated. Those included "two unique, specific prompts" made to ChatGPT and "unique responses generated by ChatGPT." For example, the suspect disclosed to

the investigator that he had asked ChatGPT to speculate on "what would happen if sherlock holmes met q from star trek?" The suspect also provided ChatGPT's response to the investigator. With the aim of identifying the suspect, federal prosecutors obtained a warrant specifying the suspect by reference to the ChatGPT prompt about Sherlock Holmes and Q, which it said was made "on about April 18, 2025." The warrant also used ChatGPT's responses to specify the user. The warrant further compelled the company OpenAI to disclose the user's names, account credentials, session histories, IP addresses, and other identifying information for April 2025.

At the time of this writing, it does not appear that federal courts have issued any binding decisions on reverse chatbot warrants specifically. Courts have diverged on the constitutionality of reverse warrants in other contexts. In April 2026, the Supreme Court heard oral arguments in *Chatrie v. United States*, on the constitutionality of geofence warrants. Depending on how the Court resolves *Chatrie*, it may shed light on at least two legal issues relevant to reverse warrants for chatbot user data. The first is the same threshold question discussed above: whether there is a reasonable expectation of privacy in the user data at issue. Although *Chatrie* focuses on Google Location History information rather than chatbot user data, the opinion could be relevant if it further clarifies *Carpenter* and the limits of the third-party doctrine. The second question that the Supreme Court might reach in *Chatrie* is whether a reverse warrant is legally sufficient for Fourth Amendment purposes. In 2024, the U.S. Court of Appeals for the Fifth Circuit held that a geofence warrant was invalid for Fourth Amendment purposes because it "amounted to a 'general' warrant prohibited by the Fourth Amendment." General warrants are those that leave too much discretion for executing officials to engage in "general, exploratory rummaging."

## Law Enforcement Use of AI for Surveillance (e.g., Vehicle Information)

The potential for AI systems to be used for mass surveillance garnered widespread attention following a 2026 dispute between the federal government and Anthropic (an AI company). As another CRS product explains, that dispute reportedly centered in part on Anthropic seeking to limit its AI products from being used for mass domestic surveillance by the government.

Depending on the context, surveillance can potentially involve a variety of law enforcement techniques ranging from wiretaps to the collection and analysis of bulk data. The precise legal issues implicated by the use of AI for surveillance will depend on the type of surveillance and the context of the use.

So far, case law on AI and surveillance remains in its nascency, and that limited body of jurisprudence has sometimes focused on the possible Fourth Amendment ramifications of AI in the context of ALPRs. ALPRs are "camera systems that capture the license plate data of vehicles, along with related information." Although the details vary, "information obtained from ALPR systems may be included in certain databases." Law enforcement agencies employ ALPRs for purposes such as evidence gathering and identifying potential suspects, among others.

At least some ALPRs reportedly employ AI for functions such as reading license plates or selecting the "best photo" to upload to a database. One private ALPR company states that law enforcement customers can use AI-powered search tools to automatically look for images of "vehicles with unique characteristics," using search phrases like "white F-150 with a ladder in the back."

Thus far, federal courts have generally rejected Fourth Amendment challenges to law enforcement's use of ALPRs. Some of those cases have focused on the underlying collection of ALPR data, typically concluding that there is no protected privacy interest in license plates displayed in plain view. Other cases focus on law enforcement access to ALPR databases, generally rejecting the contention that ALPR data should be subject to the same protections as the historical CSLI at issue in *Carpenter*.

Some courts have cautioned, however, that technologically-advanced ALPR systems could still violate the Fourth Amendment moving forward. One federal district court judge considered the potential impact of AI on ALPRs, writing:

> [L]ower court acceptance of ALPR databases leaves serious doubt about the point, if any, at which governmental use of cameras crosses the line to an impermissible warrantless search and whether linking images to a larger network or enhancing them through the use of artificial intelligence or other emerging technologies leads to a different result. Such surveillance could become too intrusive and run afoul of *Carpenter* at some point. But when?

Other federal judges have offered similar sentiments, at least in passing.

Although these courts have yet to identify a precise line where AI-powered ALPRs might run afoul of the Fourth Amendment, two potential areas of tension could "involve sustained tracking of a particular defendant through ALPRs, or an increase in the comprehensiveness of ALPR data." For example, in a case rejecting a Fourth Amendment challenge to footage from a pole camera, a federal appellate court acknowledged that there could be additional Fourth Amendment concerns if pole-camera surveillance were used "over longer periods . . . [or] in combination with other tools—such as facial recognition, automated tracking or artificial intelligence—to build a far more comprehensive portrait of an individual's life."

Courts have concluded that "comprehensive" technology-aided surveillance programs violated the Fourth Amendment in other contexts. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, for instance, the *en banc* Fourth Circuit concluded that "*Carpenter* prohibited the warrantless use of aerial surveillance to record an enormous swath of Baltimore over 12 hours daily." There, the court focused on the volume and detail of the data at issue, which it said provided exactly the type of "intimate window" into a "person's associations and activities" that *Carpenter* counseled against.

# Congressional Considerations

The two emerging issues described in this product are unlikely to be the only Fourth Amendment questions prompted by the widespread adoption of AI. If so, AI would join a long line of technological advancements like electronic eavesdropping, GPS tracking, thermal imaging, and wiretapping that, when adopted by law enforcement, have sometimes resulted in legal tension with constitutional privacy protections. Some federal judges have suggested that Congress could enact new privacy legislation in light of the potential civil liberties implications of developing technologies. Augmenting Fourth Amendment protections is a path Congress has taken in some contexts. The SCA, discussed above, is one example through which Congress sought to achieve "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." On the one hand, it protects information that in some situations would otherwise be unguarded by the Fourth Amendment due to the third-party doctrine. On the other hand, it creates a framework for law enforcement agencies to access that information when they obtain the requisite level of process. Beyond the digital realm, Congress enacted the Privacy Protection Act, which "limits the ability of federal, state, and local officials to conduct certain searches and seizures implicating First Amendment activities." Congress could also leave resolution of any Fourth Amendment issues posed by AI to the courts.

**Additional CRS Resources Relevant to the Fourth Amendment and Technology**

- CRS Report WPD00172, *Search Me! Episode 1: Advances in DNA Investigations and the Fourth Amendment*, by Jonathan M. Gaffney and Peter G. Berris (2026)
- CRS Report R48852, *Geofence and Keyword Searches: Reverse Warrants and the Fourth Amendment*, by Peter G. Berris and Clay Wild (2026)
- CRS Legal Sidebar LSB11393, *The Fourth Amendment Meets the Fourth Estate: Law Enforcement Searches of Journalists*, by Cassandra J. Barnum and Peter G. Berris (2026)
- CRS Legal Sidebar LSB11274, *Geofence Warrants and the Fourth Amendment*, by Peter G. Berris and Clay Wild (2026)
- CRS In Focus IF13068, *Automated License Plate Readers: Background and Legal Issues*, by Peter G. Berris, Kristin Finklea, and Dave S. Sidhu (2025)
- CRS Legal Sidebar LSB11339, *Advances in DNA Analysis: Fourth Amendment Implications*, by Peter G. Berris (2025)
- CRS Legal Sidebar LSB11165, *Disrupting Botnets: An Overview of Seizure Warrants and Other Legal Tools*, by Peter G. Berris (2024)
- CRS Report R48160, *Law Enforcement and Technology: Use of Automated License Plate Readers*, by Kristin Finklea (2024)

## Author Information

Peter G. Berris
Legislative Attorney

## Disclaimer