Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

COVID-19, Digital Surveillance, and Privacy: Fourth Amendment Considerations

April 16, 2020

As COVID-19 has spread across the globe, countries like South Korea and Israel have employed digital surveillance measures using cell phone location data, among other things, in an effort to track and limit the virus's transmission. In the United States, the federal government and some state and local governments have reportedly begun to gather geolocation data voluntarily provided by the mobile advertising industry to assess how people are continuing to move and congregate during the pandemic. Technology companies such as Google and Facebook have also discussed leveraging some of their aggregated and anonymized location data for similar purposes. Moreover, the recently passed CARES Act provides, as part of new funding for the Department of Health and Human Services' Centers for Disease Control and Prevention (CDC), that the CDC must report to Congress within 30 days on "the development of a public health surveillance and data collection system for coronavirus." In light of these developments, some commentators have speculated about the potential in the United States for more invasive, obligatory data collection and tracking practices emulating the measures taken in some other parts of the world.

Actions by the federal or state governments to surveil U.S. citizens in response to the COVID-19 pandemic could raise a host of legal issues, but as one commentator recently recognized, the Fourth Amendment to the U.S. Constitution may "determine the outer bounds of permissible surveillance at the federal and state levels" in this context. This Sidebar accordingly provides an overview of the Fourth Amendment and certain relevant doctrines and exceptions before discussing how the relevant legal frameworks could apply to coronavirus-related government surveillance.

Fourth Amendment Overview

The Fourth Amendment to the United States Constitution protects against "unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause," among other things. The Supreme Court has recognized that the fundamental purpose of the Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Though often discussed and applied in the context of law enforcement efforts to obtain evidence of criminal wrongdoing, and though such efforts often must satisfy stricter requirements than in other contexts, "[i]t is well settled that the Fourth Amendment's protection extends beyond the sphere of criminal

Congressional Research Service
https://crsreports.congress.gov
LSB10449

investigations." As the text of the constitutional provision suggests, the question of whether official action has run afoul of the Amendment's dictates entails consideration of at least two distinct analytical components: (1) the existence of a search or seizure, and (2) the reasonableness of that search or seizure.

Existence of a Search and the Third-Party Doctrine

A Fourth Amendment "search" can occur either when government agents physically intrude on a "constitutionally protected area" or, even absent a physical trespass, when officials violate a person's "reasonable expectation of privacy." In simple terms, absent a physical intrusion on a constitutionally protected area, "[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, . . . official intrusion into that private sphere generally qualifies as a search . . . ."

As an outgrowth of the jurisprudential focus on the "reasonable expectation of privacy," a line of cases from the 1970s developed what is known as the "third-party doctrine." The broad proposition for which these cases stand is that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Recognition of this principle led the Supreme Court in *United States v. Miller* to conclude that the government's subpoena of a suspect's bank records did not constitute a Fourth Amendment search, as the documents contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." The Court appeared to take an expansive view of the third-party doctrine in *Miller*, expounding that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." Thus, the Court held that the Fourth Amendment does not prohibit the government from obtaining information revealed to a third party even if it is assumed that "the confidence placed in the third party will not be betrayed."

Following *Miller*, the Court applied the same principles in the context of information conveyed to a telephone company in *Smith v. Maryland*. The Court in *Smith* ruled that the government's acquisition of outgoing phone numbers dialed on a landline telephone was not a search, reasoning that telephone subscribers know the numbers they dial are used by the telephone company "for a variety of legitimate business purposes." As such, when Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business" and consequently "assumed the risk" that the company's records would be divulged.

In its 2018 decision in *Carpenter v. United States*, however, the Court appeared to retreat from a broad conception of the third-party doctrine, at least as applied to certain kinds of digital information held by third-party companies. *Carpenter* involved the compelled disclosure by wireless carriers of customers' historical "cell-site location information" (CSLI), which is essentially a historical log of a cell phone's connections to geographical network access points. Law enforcement can use CSLI to determine a cell phone's location over time with a relatively high degree of accuracy. The *Carpenter* Court held that, given the "unique nature of cell phone location records," "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." The Court emphasized that the doctrine requires consideration of "the nature of the particular documents sought." On this basis, the Court distinguished prior third-party-doctrine cases as involving "limited types of personal information," pointing out that the information and documents at issue in *Miller* and *Smith* were "not confidential communications" or otherwise revealing of highly private affairs. By contrast, the *Carpenter* Court viewed it as significant that CSLI "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." The Court also discounted one of the rationales underlying the third-party doctrine—that information has been voluntarily exposed—in the case of CSLI, writing that such information "is not truly 'shared' as one normally understands the term" because "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up." For these reasons, the Supreme Court concluded that the government's acquisition of customer cell-

site records from third-party carriers was a search within the meaning of the Fourth Amendment. Nevertheless, the Court characterized its ruling as a narrow one, noting that it did "not disturb the application of *Smith* or *Miller*, call into question" other surveillance tools like security cameras, address "other business records that might incidentally reveal location information," or consider "collection techniques involving foreign affairs or national security."

Reasonableness and Special Needs

Once it is established that a Fourth Amendment search has occurred, the question becomes whether that search was "reasonable." Whether a particular class of searches meets the reasonableness standard may depend on context. Where a search is conducted "by law enforcement officials to discover evidence of criminal wrongdoing," and subject to "a few specifically established and well-delineated exceptions," reasonableness ordinarily requires that the government first obtain a judicial warrant based on probable cause before a search can occur. For instance, after concluding that the acquisition of CSLI from third-party carriers in *Carpenter* was a Fourth Amendment search, the Court applied the general rule and held that "police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation[.]"

That said, neither a warrant nor probable cause is "required to establish the reasonableness of *all* government searches." Among other things, the warrant and probable cause requirements may be inapplicable "when special needs, beyond the normal need for law enforcement," make those requirements "impracticable." Such special needs may include, for example, the need to maintain order in the public school context or "the operational realities of the [public] workplace." In cases where the Court has applied the so-called "special needs" doctrine, it has generally balanced the individual and governmental interests at issue, focusing on a variety of factors. These factors have included the scope of the privacy interest at stake, the degree of intrusion on that interest, the immediacy and significance of the governmental concern, and the efficacy of the intrusion in meeting the concern. Though the circumstances in which this "special needs" doctrine may apply defy easy categorization, when the factors tip the balance in favor of the government, searches or seizures without a warrant and even without any individualized suspicion of wrongdoing—like sobriety checkpoints or random drug testing in some situations—may be considered reasonable and thus comport with the Fourth Amendment. The Supreme Court has specifically noted in this regard that a "risk to public safety [that] is substantial and real" may justify "blanket suspicionless searches calibrated to the risk," citing as examples the routine searches conducted at airports and entrances to some official buildings.

One apparent strand of the "special needs" doctrine is a category of cases in which courts have upheld searches conducted pursuant to legislative or administrative regulatory regimes—such as those that may apply to probationers or in certain industries—without the need for a warrant supported by probable cause. At least in circumstances that are sufficiently distinct from ordinary law enforcement, courts have sometimes employed a balancing test similar to the one described above where "reasonable legislative or administrative standards" are in place to preclude arbitrariness.

Application to Potential COVID-19-Related Surveillance

Assuming the federal or a state government is involved in efforts to surveil or track the movements of U.S. citizens in response to the COVID-19 pandemic, the first question for purposes of constitutional analysis would be whether such efforts amount to a Fourth Amendment search, which could depend on the means, source, and scope of the information sought or obtained. The use of traditional surveillance devices such as security cameras to monitor compliance with stay-at-home orders, for instance, might not implicate constitutional concerns if limited to public locations for a brief period of time, as such devices may not "present the kind of aggregate view of intimate details of" a person's movements that concerned the Court in *Carpenter*. Additionally, monitoring through mobile apps or other means, such as opt-in

Bluetooth contact tracing that does not rely on location data, could be seen by a court as unobjectionable if voluntary in nature and limited in scope. However, a government effort to acquire information more akin to the circumstances of *Carpenter*—i.e., compelled provision of location data on specific individuals from companies in possession of the information—might present a closer question. Though third-party doctrine precedent prior to *Carpenter* would suggest that exposure of information to third-party companies could negate any reasonable expectation of privacy in that information, the Court in *Carpenter* made clear that it intends to view its precedent and the doctrine flexibly in the face of "seismic shifts in digital technology" that give third parties access to vast swaths of information revealing "the privacies of life."

Assuming the existence of a Fourth Amendment search, the constitutionality of government surveillance or data collection efforts would depend upon the reasonableness of the search. This inquiry is fact-bound and ultimately dependent on the context in which the search takes place. Efforts to obtain at least some kinds of location information as evidence of criminal wrongdoing for purposes of ordinary law enforcement could require a warrant based on probable cause unless an exception existed (e.g., if exigent circumstances, such as preventing imminent harm, negated the need for a warrant).

Beyond the context of ordinary law enforcement, it might be argued that containment of a deadly virus constitutes a special need that could justify some form of warrantless, suspicionless surveillance or data collection. There is some authority to support the proposition that preventing the spread of a communicable disease could be considered a special need under the Fourth Amendment in certain circumstances. A court faced with such an argument would likely balance the individual and governmental interests at issue as described above, which would involve fact-specific consideration of the scope of the intrusion (e.g., anonymized contact tracing or acquisition of limited kinds of personal information versus broader surveillance or acquisition of precise location data over time) as well as the government's concern. In this latter regard, given the Supreme Court's recognition that a substantial "risk to public safety" may justify calibrated suspicionless searches, a court could view the balance as tipping in favor of government surveillance while the COVID-19 pandemic is ongoing. That said, because of how fact-dependent the special needs analysis is, it is difficult to say with certainty how a court would rule. Even cases involving the same type of privacy interest and incursion—such as drug testing—have produced disparate results depending on the other factors a court may consider.

Given the highly fact-specific and fluid nature of the relevant constitutional doctrines, as well as the privacy and governmental interests at stake, Congress may consider whether to act. Congress might attempt to establish standards for governmental acquisition of digital-location or other kinds of information in response to the COVID-19 pandemic, which could factor into a court's analysis of reasonableness. That said, Congress may not legislate away constitutional protections, and thus any legislative framework authorizing suspicionless searches would need to be sufficiently "calibrated" to the ostensible special needs of disease detection and spread prevention. Existing federal and state laws may also regulate the government's ability to obtain and use certain kinds of personal information related to the pandemic. Congress could impose further statutory limits if it perceives the protections of the Fourth Amendment or existing laws to be lacking in this context, as it has done with respect to the contents of electronic communications held by certain kinds of third-party companies, though there would remain the possibility that statutory limits could be superseded by an intervening judicial decision interpreting the Constitution.

Author Information

Michael A. Foster
Legislative Attorney

Disclaimer