Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Abortion, Data Privacy, and Law Enforcement Access: A Legal Overview

July 7, 2022

In light of the U.S. Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, some Members of Congress and commentators have expressed concerns that law enforcement officials may seek to collect abortion-related personal data for prosecutions in states that have criminalized abortions. In *Dobbs*, the Court overruled *Roe v. Wade* and held that the U.S. Constitution does not grant individuals a right to an abortion. States now have much more discretion to criminalize abortion. Moreover, in the years before the *Dobbs* decision, 13 states passed "trigger laws" that were set to prohibit abortion, either automatically or following action by a state official, if the Supreme Court overturned *Roe*. Various types of personal data—such as health records, financial records, geolocation information, and electronic communications—might shed light on an individual's abortion decision, and law enforcement could seek such information, either directly from the entity collecting the data or from another entity to whom the data has been shared or sold.

Federal law may affect law enforcement's ability to collect this information. The Fourth Amendment to the U.S. Constitution generally requires law enforcement officials to obtain a warrant before collecting personal data, although this requirement typically does not apply when the information is held by a third party. Beyond the Constitution, federal privacy statutes create disclosure protections for some categories of personal data, such as healthcare data, financial data, and electronic communications. Many entities not subject to these specific federal privacy statutes may still collect, directly or indirectly, data relevant to an individual's abortion decision, such as their geolocation data or web browsing activity. Data brokers, for example, collect a broad range of data on individuals and often resell those data. While not subject to any bright-line statutory privacy rules, these entities are still subject to the Federal Trade Commission Act's (FTC Act's) broad prohibition on "unfair and deceptive acts or practices."

This Legal Sidebar provides a high-level survey of the relevant constitutional and statutory law on this topic, and it concludes with considerations for Congress and links to other relevant CRS products.

The Fourth Amendment

The Fourth Amendment prohibits federal and state officials from conducting "unreasonable searches and seizures." Under Supreme Court case law, a "search" may be unreasonable, even when there is not a

Congressional Research Service
https://crsreports.congress.gov
LSB10786

physical intrusion, if the official violates an individual's reasonable expectation of privacy. For a search to be considered reasonable, outside of some specific exceptions, the official must obtain a search warrant from a court based on probable cause. The Fourth Amendment's protections against unreasonable searches and seizures seldom apply when the official is collecting information about an individual from a third party. For example, the Court has held that the Fourth Amendment's protections did not apply when law enforcement is seeking a suspect's financial records maintained by a bank or phone records showing the phone numbers the suspect has dialed. The rationale behind this third-party doctrine is that, by sharing their information with a third party, such as a bank or a telephone provider, the individual no longer has a reasonable expectation of privacy in that information.

On the other hand, the Court recognized a limitation to the third-party doctrine in the 2018 case *Carpenter v. United States*. In *Carpenter*, law enforcement collected a large volume of customers' historical cell-site location information (CSLI) from cell phone providers, which showed the suspect's detailed movements over the course of 127 days. The Court held that this information was protected by the Fourth Amendment, despite being maintained by phone providers. The Court emphasized that the data collection was a necessary byproduct of consumers' cell phone usage, which itself is "indispensable to participation in modern society." The Court said that there is a "world of a difference" between the bank records and call records in its prior third-party doctrine cases and the "exhaustive chronicle of location information" that showed a person's physical presence "every day, every moment" over a long period of time. The Court presented this decision as an extension of a prior line of cases discussing a person's reasonable expectation of privacy in their physical location and movements, where a majority of the Court agreed that the Fourth Amendment would protect against law enforcement surreptitiously using GPS tracking to conduct extended and comprehensive surveillance of a person's movements.

In the abortion context, the Fourth Amendment's protections against unreasonable searches and seizures would apply whenever law enforcement is gathering information directly from the individual who has a reasonable expectation of privacy in it. For example, before confiscating an individual's cell phone and reviewing text messages or other evidence of an individual's abortion decision, law enforcement would likely need to first obtain a search warrant. On the other hand, if law enforcement collects abortion-related records from a third party, such as records from a health care provider or financial institution, it would likely fall under the third-party doctrine and not be considered a "search." However, the third-party doctrine may not apply to a situation with similar characteristics as *Carpenter*, such as where law enforcement seeks exhaustive location information from a third party that tracks an individual's movements over a long period of time, particularly if that information has been gathered by virtue of the individual's use of a technology that has been deemed essential to participation in modern society, and where the technology does not meaningfully permit the consumer to opt out of the collection and storage of the relevant data. Even when the Fourth Amendment applies and law enforcement must seek a warrant in court, the Fourth Amendment may still limit the scope of the warrant. For example, a federal district court recently held that a "geofence" warrant, which directed Google to turn over location information for all devices that entered a defined location within a specified time frame, was invalid because the government had not shown there was probable cause to believe that all of the accounts sought were associated with persons involved in the crime.

Relevant Privacy Statutes

Although the Fourth Amendment may be largely inapplicable when law enforcement gathers information from third parties, federal privacy statutes may govern or limit law enforcement's access to this data. Many of these statutes apply to specific types of data held by particular entities, such as healthcare data, financial data, electronic communications, and personally identifiable records held by federal agencies. These privacy statutes typically prohibit covered entities from disclosing protected data to third parties without the individual's consent or opportunity to opt out of the disclosure. These laws generally have

law enforcement exceptions, however, enabling covered entities to disclose, without consumer consent, data to law enforcement officials pursuant to a warrant, subpoena, or other legal process. Beyond these targeted privacy laws, the FTC Act serves as a catch-all standard that allows the Federal Trade Commission (FTC) to address privacy practices by a broad range of entities.

Health Information Portability and Accountability Act: Healthcare Information

The main law protecting health information is the Health Information Portability and Accountability Act (HIPAA). HIPAA and its implementing regulations require covered entities (healthcare providers, health plans, and healthcare clearing houses) and their business associates to comply with various data privacy and data security requirements (known respectively as the HIPAA Privacy and Security Rules). Most relevantly, the HIPAA Privacy Rule generally prohibits covered entities from sharing an individual's identifiable health information to third parties without the individual's authorization, other than disclosures for treatment, billing, or health care operations. However, the Privacy Rule also includes several exceptions to this general prohibition on sharing, including a law enforcement access exception. Under this exception, covered entities may disclose health data to law enforcement officials pursuant to a court order or warrant, a grand jury subpoena, or an administrative subpoena meeting certain conditions. Additional exceptions may also be relevant, including the exception allowing a covered entity to disclose health information that is evidence of criminal activity that occurred on its premises and health information that it believes in good faith to be necessary to avert or lessen a serious and imminent threat to the health or safety of a person or the public.

The Gramm-Leach-Bliley Act and Right to Financial Privacy Act: Financial Information

Financial records, such as charges at abortion clinics, might also be relevant to abortion investigations or prosecution. Two key statues govern the privacy of financial records: the Gramm-Leach-Bliley Act (GLBA) and the Right to Financial Privacy Act (RFPA). The GLBA generally prohibits financial institutions from disclosing a consumer's financial information to third parties without first notifying the consumer and allowing them to opt out of the disclosure. The GLBA also has a law enforcement exception. Financial institutions do not have to follow the notice-and-opt-out requirement if they are responding to a "properly authorized" civil, criminal, or regulatory investigation or subpoena or summons from a federal or state law enforcement authority.

The RFPA contains additional privacy protections that apply to federal law enforcement investigations. Generally, the RFPA prohibits financial institutions from disclosing financial records to federal law enforcement officials unless the official obtains a warrant, judicial subpoena, administrative subpoena, formal written request authorized by regulation, or national security letter. It also requires at times that the individual whose records are being sought be given notice and an opportunity to challenge the disclosure in court. While the RFPA only applies to federal law enforcement officials, it might be relevant if, for example, a federal law is enacted criminalizing abortions. Federal investigations may also occur if the Department of Justice changes its current position and prosecutes federal employees performing abortions under the Assimilative Crimes Act (which generally makes it a federal crime to violate state law on federal land).

The Stored Communications Act: Electronic Communications

Text messages, emails, and private messages over social media platforms or other platforms might provide evidence of an individual's abortion decision and might be sought by law enforcement. The

Stored Communications Act (SCA) is the primary law that restricts tech companies from disclosing electronic communications like emails or social media messages, as well as non-content customer records. The SCA applies to "electronic communications services" (ECS) (such as cell phone providers, email providers, or social media platforms) and "remote computing services" (RCS) (such as cloud computing providers). The SCA restricts these entities from disclosing the contents of electronic communications to federal and state law enforcement officials. Absent customer consent or another discrete exception, an RCS may generally disclose the contents of an electronic communication only if the law enforcement official obtains a court-issued warrant, or, with notice to the customer, a court order issued under procedures laid out in the Act or an administrative subpoena. For electronic communications held by an ECS for 180 days or less, only a court-issued warrant is sufficient. To access other kinds of non-content customer records held by an ECS or RCS, law enforcement generally must obtain a search warrant, a court order, or a subpoena, depending on the circumstances.

The SCA also restricts disclosures to non-law enforcement third parties. ECSs and RCSs may generally only disclose the contents of an electronic communication if either the sender or recipient of the communication gives authorization. The SCA does not, however, restrict an ECS or RCS from disclosing non-content information about a customer's communication (such as the IP address of the device used to send the communication).

The Privacy Act: Data Held by Federal Agencies

At times, a federal agency may obtain an individual's abortion-related data. For instance, the Veterans Benefits Administration (VBA) in the Department of Veterans Affairs (VA) might obtain a veteran's abortion-related data in connection with a claim for VA benefits. VBA—unlike VA's Veterans Health Administration—is not subject to HIPAA. Another privacy law, however, applies generally to federal agencies: the Privacy Act of 1974. The Privacy Act applies to how agencies treat certain "records" that contain an individual's personal information. The Privacy Act generally prohibits federal agencies from disclosing these records without the individual's consent, unless an exception applies. There is an exception for disclosure to law enforcement for civil or criminal law enforcement purposes, but for the exception to apply, the head of the law enforcement "agency or instrumentality" must make a written request that specifies the particular portion of the record desired and the relevant law enforcement activity. Even if a record falls under the Privacy Act's law enforcement exception, the agency may be able to voluntarily withhold it. The Privacy Act only *requires* disclosure if the individual who is the subject of the record is the one requesting it. Other laws, however, like the Freedom of Information Act (FOIA), may require disclosure if the proper procedures are followed.

The FTC Act: Non-HIPAA Health Data, Geolocation Data, and Other Commercial Data

There are many commercial data practices that fall outside the scope of the various statutes mentioned above. For instance, non-HIPAA covered entities, such as health smartphone applications (apps) and wearable fitness trackers, might track menstrual cycles or collect other health information. Other smartphone apps might collect users' geolocation data. Data brokers collect troves of data on individuals that are compiled from various sources to resell that data. Such activities, while generally not regulated by any specific privacy statute, are still subject to the FTC Act. The FTC Act prohibits "unfair or deceptive acts or practices" in commerce, and it is enforced by the FTC. While the FTC Act does not contain any bright-line restrictions or prohibitions on companies' disclosure of personal information to law enforcement or third parties, the FTC has brought enforcement actions against companies that mislead consumers about their data disclosure practices. Some Members of Congress have recently called on the FTC to use this authority to investigate data practices that might disclose an individuals' abortion-related

activity, specifically asking the Commission to investigate Apple's and Google's collection and sale of consumers' movements and web browsing activity.

Considerations for Congress

As explained above, federal data privacy law provides relatively limited constraints upon law enforcement's ability to acquire privacy data relating to criminal activity, potentially including abortion activity proscribed under the state laws of the requesting law enforcement agency. Although Fourth Amendment caselaw recognizes some limits on law enforcement's ability to acquire third-party data, those limits seem unlikely to be triggered by requests for information related to a suspect's criminal activity, except if that information enabled the government to engage in prolonged surveillance of the suspect. Numerous federal statutes place limits on information access, but most include carve-outs for law enforcement requests.

Should Congress want to build on or change the current mix of statutory requirements, one approach might be to enact a standalone law specifically addressing the treatment and disclosure of abortion-related data. For example, while it does not specifically address disclosure to law enforcement, the My Body, My Data Act of 2022 (H.R. 8111/S. 4454) would create various privacy protections for "personal reproductive or sexual health information," including a requirement that entities only collect and use these data if the individual has consented or if they are strictly necessary to provide a service or product that the individual has requested. Another approach might be for Congress to address this issue as part of a comprehensive privacy bill, such as the American Data Privacy and Protection Act (ADPPA) (H.R. 8152). The ADPPA would create a comprehensive federal consumer privacy framework, including giving consumers various rights to access, correct, and delete their data held by covered entities. It also would require, absent a specific exception, that entities obtain a consumer's consent before transferring their "sensitive covered data" (which includes, among other things, health information, geolocation information, and private communications) to a third party. The ADPPA does not explicitly specify how this consent requirement would apply to disclosures to law enforcement. Other proposals introduced in the 117th Congress that would prohibit or limit the government's ability to obtain communications information from third parties include the Fourth Amendment Is Not For Sale Act (H.R. 2738/S. 1265), which would prohibit law enforcement and intelligence agencies from purchasing communications data from data brokers.

Other CRS Products

CRS Legal Sidebar LSB10768, *Supreme Court Rules No Constitutional Right to Abortion in Dobbs v. Jackson Women's Health Organization*, by Jon O. Shimabukuro

CRS Legal Sidebar LSB10779, *State Laws Restricting or Prohibiting Abortion*, by Laura Deal

CRS Legal Sidebar LSB10157, *UPDATE: Supreme Court Takes Fourth Amendment Case about Cell Phone Location Data*, by Ben Harrington

CRS Legal Sidebar LSB10449, *COVID-19, Digital Surveillance, and Privacy: Fourth Amendment Considerations*, by Michael A. Foster

CRS Report R45631, *Data Protection Law: An Overview*, by Stephen P. Mulligan and Chris D. Linebaugh

CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle

CRS Legal Sidebar LSB10776, *Overview of the American Data Privacy and Protection Act, H.R. 8152*, by Jonathan M. Gaffney, Eric N. Holmes, and Chris D. Linebaugh

Author Information

Chris D. Linebaugh
Legislative Attorney

Disclaimer