CHAMBER OF PROGRESS

July 13, 2022

The Honorable Merrick B. Garland
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Attorney General Garland,

We write to request that the Department of Justice update its current position on the privacy of electronic communications data and content under the Fourth Amendment, to ensure that state law enforcement agents are not able to invade women's most personal data without adequate constitutional safeguards.

In the wake of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, President Biden called on the Administration to take action to protect a woman's right to choose. As you recognized in your June 24, 2022 statement on *Dobbs*,[1] women have the right to travel to obtain legal abortions, but women who chose to do so – and reproductive health organizations that provide information and assistance to women – may still face the threat of state criminal prosecution.

The President's July 8, 2022 Executive Order on Protecting Access to Reproductive Healthcare Services called on you "[t]o address the potential threat to patient privacy caused by the transfer and sale of sensitive health-related data and by digital surveillance related to reproductive healthcare services,"[2] but did not not address the privacy risks posed by law enforcement access to data.

Stronger action is needed to protect women's right to choose from state law enforcement witch hunts. In particular, there needs to be strong constitutional protection for our most private data from unjustified law enforcement intrusions.

Women need to be able to access the Internet and mobile devices to search, arrange, and travel for reproductive health services. Online service providers can take certain actions to help protect the privacy of women seeking reproductive health services, but have limited ability to deny law enforcement access to data.

---

[1] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-statement-supreme-court-ruling-dobbs-v-jackson-women-s

[2] Executive Order on Protecting Access to Reproductive Healthcare Services, Section 4(b).

The ability of state law enforcement to compel online service providers to disclose this type of information puts women in an impossible position of having to choose between exercising their reproductive rights and avoiding creating evidence that could lead to their criminal prosecution under a state law that restricts those rights.

The DOJ plays an instrumental role in setting the legal precedent and interpretations of how the Fourth Amendment applies to the modern technologies that pervade our lives. Lawyers within the Criminal Division, the investigative agencies under the DOJ umbrella, and in US Attorney Offices around the country advise investigators and make legal arguments in criminal prosecutions that create precedents on the application of statutory and constitutional protections to electronic data.

Unfortunately, federal prosecutors have repeatedly made arguments that undermine the Fourth Amendment protections for data held by third party service providers. These arguments are often unnecessary to successful prosecution of the criminal defendants and pose a significant threat to the Fourth Amendment rights of women who live in jurisdictions that restrict their reproductive rights. For example:

- **Cell Site Location Information:** Despite the Supreme Court's ruling in *Carpenter v. United States* that the fact that data is held by a third party provider does not automatically cause cell site location information ("CLSI") to lose its Fourth Amendment protections, federal prosecutors regularly fight the application of *Carpenter's* rationale to CSLI.[3] In reproductive rights cases, this would allow state law enforcement to easily and lawfully monitor the real-time locations of women they suspect may seek an abortion.

- **Third Party Doctrine:** In addition to fighting the application of the Supreme Court's *Carpenter* ruling to CLSI, federal prosecutors also still argue that third party doctrine precludes Fourth Amendment protection for additional types of data held by service providers, including email.[4] In the reproductive rights context, this would allow state law enforcement to rummage through a woman's personal correspondence containing health information with no judicial oversight.

- **Terms of Service:** Federal prosecutors also routinely argue that service provider terms of service vitiate a consumer's "reasonable expectation of privacy" resulting in loss of Fourth Amendment protection from warrantless law enforcement intrusions. Given that most online service providers have terms of service, this would render everything from a women's calendar showing her medical appointments to her text message history with counselors available to state law enforcement with a simple subpoena.

[3] *See, e.g.*, *USA v. Baker et al*, 3:19-cr-00032, No. 139 (M.D.Pa. May. 4, 2021)(arguing that real-time acquisition of CSLI is not a search under the Fourth Amendment).
[4] *See, e.g.*, *USA v. Luke Wilson*, 18-50440, No. 29 (9th Cir. Jun. 21, 2019).

The rising use of "geofence" warrants by state law enforcement shows how dangerous these arguments can be to the rights of women against warrantless privacy intrusions by law enforcement.[5]

Geofence warrants allow law enforcement to identify all individuals who were in a particular vicinity in a particular window of time. States that criminalize abortions could easily apply this investigative technique to target reproductive health organizations and clinics that may advise women on the availibility of abortion services in other states or to create a dragnet to identify women who may seek reproductive services out of state.

In the recent case *U.S. v. Chatrie*, federal prosecutors argued that *Carpenter*'s protections for CSLI did not apply to the data collected through use of a geofence warrant issued to Google, even though the location information was more precise than CLSI. In fighting the defense's suppression motion, federal prosecutors repeatedly invoked the third party doctrine to support their argument that the defendant had no Fourth Amendment rights in the location information disclosed to a service provider.[6] This argument was advanced even though the search at issue was conducted pursuant to a warrant and the officer's good faith reliance on the validity of the warrant made suppression of the evidence unlikely.

Under the arguments advanced by the Department of Justice in recent cases, a warrant would be unnecessary and the only specific protections would be those supplied by federal and state statutes, most of which allow access to data on a standard lower than probable cause, do not impose particularity requirements, and may not require (or even allow) judicial scrutiny.[7]

DOJ's approach to these issues is highly influential. Courts have already adopted the government's reasoning that individuals do not have a reasonable expectation of privacy in electronic data and communications held by service providers.[8]

We share your interest in successful prosecution of dangerous criminals, but believe that interest is compatible with recognizing that important constitutional protections must apply to Americans' most personal information regardless of whether it is located in their home, on their phone, or held by a service provider. In the absence of strong statutory protections, women depend on these constitutional guarantees to protect their privacy from state law enforcement's unwarranted intrusions.

---

[5] *United States v. Chatrie*, 3:19cr130, at 17 (E.D. Va. Mar. 3, 2022)(citing Google, Supplemental Information on Geofence Warrants in the United States, https://bit.ly/3o7Znqc.)(showing rise in usage of geofence warrants and that federal warrants only comprise 4.4% of such warrants); see also, Brief of Amicus Curiae Google Inc., *Id.*, No. 73, at 3 (E.D.Va. Dec. 23, 2019)(noting Google observed a 1500% increase in use of Geofence warrants from 2017 to 2018 and a 500% increase from 2018 to 2019).
[6] *Id.*, No. 41 (November 19, 2019), No. 109 (June 12, 2020), No. 214 (June 17, 2021).
[7] *See, e.g.*, the federal Pen Register Trap and Trace statute which states that "the court shall issue" a court order if a government lawyer makes the required certification. 18 U.S.C. § 3121(a)(1).
[8] *See, e.g.*, *United States v. Montijo*, 2:21-cr-75-SPC-NPM, *15-16 (M.D. Fla. Jan. 10, 2022); *United States v. Wolfenbarger*, No. 16-CR-00519-LHK-1, *20 (N.D. Cal. Aug. 29, 2019).

Chamber of Progress urges you to ensure the DOJ's legal activities related to the Fourth Amendment's application to personal data held by online service providers allow women to access reproductive health services – whether in their home state or another – without fear that doing so may expose their data to state law enforcement officials acting outside the requirements of the Fourth Amendment's protections.

Sincerely,

Elizabeth Banker
VP, Legal Advocacy