NINA MOINI: We're going to turn to the US Supreme Court, which will soon finish its current term by late June or early July. The justices will announce their decisions in a handful of high-profile cases. One of those has to do with how law enforcement uses the location data that's collected by tech companies. Investigators use a tool called geofencing to draw a virtual boundary around an area where a crime was committed, and find out which phones were nearby. Law enforcement needs a warrant to access this data, but critics say the tactic violates privacy rights. Joining me to explain is Julie Jonas, a law professor at the University of St. Thomas. Thanks for your time this afternoon, Professor.

JULIE JONAS: Hi thanks for having me.

NINA MOINI: For starters, would you just explain a little bit more about how geofencing works in a law enforcement context?

JULIE JONAS: Yeah. So I think you explained it for your listeners very well. What a geofence is it allows a fence, in essence, to be drawn around a certain area where and when a crime occurred. And then law enforcement can go to Google and ask Google to tell them the device numbers of any cell phones that were in that area during the time that the crime occurred. As we all know, Google and other apps are tracking us. They're using mapping.

Some of the tracking that they do is helpful, like mapping apps, but they also do it to deliver us ads. If you have an Android phone or use certain apps, even on an Apple device, that information is being collected and kept by Google in something called a Sensorvault. Google had indicated around the time the Chatrie was at the Court of Appeals that they were no longer going to store this information in the Sensorvault, but there's no indication that they've actually stopped.

But Google is interesting as opposed to other data aggregators that we can talk about in that Google required the government to have a warrant to get at this data. So it wasn't that the government on its own said that they needed to go get a warrant, but rather Google said, we're not going to give you access to this data unless you produce a warrant. And then there was a three-step process that Google developed. And in that process, and at that point in time, Google was only requiring a warrant for the first step in the process, which was law enforcement will give them a time that the crime occurred and a parameter, a fence around that area, and would ask for all the anonymized device numbers of all of the devices that were in that area at the time.

Then at the second step, where Google did not require a warrant, law enforcement was allowed to expand that search to basically narrow the data, narrow the devices that they were interested in, because many of the devices that would be in a particular area could be irrelevant. It could be somebody who was just driving through, who lived in the area, who worked in the area, who was there for legitimate reasons. So if a device stayed in the area for a longer period of time than the crime occurred, maybe it was a person who worked at the bank, for instance, as in the *Chatrie case,* or maybe it was someone who was just driving through the area, as in the contrary, *Sanchez case.*

So that's the second step, at which point law enforcement is supposed to they expand the scope of the search, but they narrow the data. And then once they've narrowed that data and done some additional investigation, they can go to Google again and ask for identifying information on the users, which is certainly their names and their email addresses or Gmail addresses, but could even expand to their search histories.

NINA MOINI: Wow! And I think it's this question now before the US Supreme Court of balancing, helping, I guess, law enforcement. A lot of people hear it and they think, well, hey, why not? If it helps people solve a crime. Let's give them all this information. But there are constitutional rights. There are laws. What are the questions that are before the US Supreme Court as it pertains to people's privacy and just rights?

JULIE JONAS: Well, the big issue comes down to do we have a reasonable expectation of privacy in where we go, in our locations throughout our day? I think most people would say, yes, we do-- that law enforcement can't use our cell phone data, and we all use our cell phones so regularly that they can't use that information to track us. Now, of course, it's wonderful as a crime-solving tool, but you can think about other ways where it could be misused to track people, to political meetings, or to abortion clinics or other health care providers.

There's been instances of companies who are not perhaps as reliable as Google is, where they sell this data to law enforcement. In one case, they used it to out a Catholic priest who was visiting gay bars. In another case, they were selling this data to the federal government using a popular Muslim dating website, as well as an app that allowed them to know the direction of Mecca when they said their daily prayers. So you can see where this is a very slippery slope. And I think Google was trying to be careful, but maybe it wasn't quite enough.

NINA MOINI: I wonder if you know about alternatives for law enforcement to get location data regardless of this ruling. Are there other ways that could preserve more privacy for people?

JULIE JONAS: No the other ways are actually worse for people because law enforcement can buy this data. There are companies out there like X-mode, and SafeGraph, Fog Data Science who are selling it to law enforcement. And because law enforcement isn't compelling them to sell it, there's no warrant requirement at all. So oftentimes, defendants and other people don't even know it's happening.

There was another situation during COVID where law enforcement actually-- well, actually it was the city of San Jose, in California used it to determine who was in that church, Calvary Church, that the government determined and had said should be shut because of COVID. Law enforcement used a geofence from a private company-- the data that they got from a private company to determine who was in the church.

NINA MOINI: And earlier in the show, if you caught our interview about yesterday's arrests of some 15 anti-ICE protesters that the government's charged with conspiracy to impede or injure federal officers. And you alluded to how geofencing might be used to collect data on people for various types of activities. Are you concerned about that and these cases, in particular, related to protest activity?

JULIE JONAS: Absolutely. I know that it was also used during the George Floyd protests in Minneapolis to try and ascertain who was in certain areas at certain times. And I suppose depending on your political persuasion, it was also used during January 6 to determine who had breached the Capitol, who was in the Capitol during that time period, who shouldn't be in there. So it can be used by whatever the government determines they want to pursue.

NINA MOINI: It sounds like this Supreme Court ruling-- I mean, as all of the rulings-- is going to have maybe implications for a lot of other areas that we've talked about just in our time together. Do you have a sense for where the Supreme Court's leaning on the geofencing case and when that ruling may come?

JULIE JONAS: Yeah. I think it will come the end of this term. I don't think that the ruling will be as broad as people would expect. I think Justice Sotomayor really tipped her hand, and I wouldn't be surprised if she had a majority of the court to go with her on this-- to simply say that the government, when requesting any geofence from Google, needs to have a warrant at every step, or at least certainly at step 3 when they ask for that deanonymized data.

And that's what the Minnesota Supreme Court just did in a recent case here, contrary to Sanchez. The Minnesota Constitution has traditionally granted us more privacy rights than the federal Constitution. And the Minnesota Supreme Court said that law enforcement had to go back to the court at each step to get a warrant, to show probable cause for the next step in the warrant, to prevent law enforcement from having unfettered discretion at each of those steps. And I wouldn't be surprised if the Supreme Court said something very similar.

NINA MOINI: All right. Julie Jonas, thanks for sharing your expertise with us. We really appreciate your time.

JULIE JONAS: Yeah. Well, thank you so much for having me. Have a nice day.

NINA MOINI: You too. Julie Jonas is a law professor at the University of St. Thomas.