Re-Drawing the Privacy Line: Chatrie's Legislative and Oversight Implications

Thu, Jul 09, 2026 12 PM

SUMMARY KEYWORDS

Supreme Court, privacy, Fourth Amendment, geolocation, warrant, law enforcement, digital data, third party doctrine, sensitive information, consumer privacy, legislative implications, data broker loophole, reverse search, technological capabilities, civil liberties.

SPEAKERS

- Jennifer **Huddleston**, Senior Fellow, The Cato Institute
- Jake **Laperruque**, Deputy Director, Center for Democracy & Technology
- Paul **Taske**, Director, Litigation Center, NetChoice
- Tim **Lordan**, Executive Director, Congressional Internet Caucus Academy

Tim Lordan 00:01

Hello, and welcome. Today we have three experts in the field joining us. To my left is Jennifer Huddleston, senior fellow in technology policy at the Cato Institute. Next to her is Paula Taske, director of the NetChoice Litigation Center. And next to Paula is Jake Laperruque, deputy director of the Security and Surveillance Project at the Center for Democracy and Technology.

We have been doing these briefings for a long time. In fact, eight years ago, in this same room — or at least I think it was this same room — we held a briefing on the predecessor to this case, *Carpenter v. United States*. Today's panel is missing one important perspective: investigators and law enforcement. Those voices can be difficult to get up here, and I was not able to secure that perspective for this panel.

So, from time to time, I may try to articulate what law enforcement would say in defense of these practices. If you hear me doing that as moderator, understand that I am trying to make sure that perspective is represented in the discussion.

The main reason we are here today is the Supreme Court's recent decision in *Chatrie v. United States*, a geolocation privacy case involving the Fourth Amendment, searches, seizures, and warrants. The facts began with a bank robbery near Richmond, Virginia. Witnesses said the robber had a cell phone, so investigators went to Google, which holds a significant amount of location information, and obtained a geofence warrant.

The initial request asked Google to identify user accounts that were within a 150-meter radius of the bank during a narrow time window — roughly half an hour before and half an hour after the robbery. That radius is about one and a half to two city blocks here in Washington, D.C. Google first provided anonymized user accounts, without names. Investigators then came back and asked for additional location information on some of those accounts over a longer time period and a broader geographic area, to see where those users had come from and where they went after the robbery. Finally, after narrowing the list to three accounts, investigators asked Google to unmask those users. One of them was Mr. Chatrie.

So the question that moved through the courts was whether this three-stage geofence warrant was specific enough and reasonable enough under the Fourth Amendment's protection against unreasonable searches and seizures. We will define the Fourth Amendment and look more closely at the text in a moment. But those are the basic facts of the case. The Court ultimately said this was a search, and that means it requires Fourth Amendment scrutiny. So let me start with Jennifer: what does it mean for the Court to say this is a search — and what follows from that?

Jennifer Huddleston 05:00
Right. So the court was basically saying that this is the type of search that the Fourth Amendment was designed to apply to, and you know, I think it's really interesting that we're having this conversation right after the 250th anniversary of the Declaration of Independence, a time when we've been thinking a lot about what the founders intended when they founded America, and it's often easy to say, well, the founding fathers never would have understood a cell phone. However, you know, look, I don't know. I think if you locked Benjamin Franklin in the room, in a room with a cell phone long enough, he would have figured it out, and that they, but they did understand these basic values around how to protect individuals' privacy and what it meant, and what we see now is the court trying to interpret those in this digital age. You heard a lot come up about how does this compare to, like, a safety deposit box, and the kind of understanding that there's a very - that there is a significant difference in the kind of geolocation or other sensitive data that may be involved in this type of case v. something that when someone is willingly giving information to a bank teller, as was traditionally seen under the under the third party doctrine.

Tim Lordan 06:14
So, Paul, let me, let me ask you, if like the fourth amendment, like I'm gonna, I'll put up the text, hopefully it works. That's the text of the Fourth Amendment. What does this say?

Paula Taske 06:24
Sure, if we, if we zoom out, the Fourth Amendment basically is at the founding one of the grievances that the then colonists and then, you know, new founding fathers had was this sort of arbitrary government overreach into the personal lives of themselves, the king could issue a search warrant, you know, basically without any factual support, and say, "Go attack that guy's house and get me the papers in there, so that we can take a look to see if he's done anything bad, and so that what the Fourth Amendment does is say, "No, no, no. In America, we are going to require that the people are going to be free from that sort of arbitrary government interference and snooping into their persons, you know, homes, papers, and effects. So we wanted to prevent that same sort of overreach in the new nation that became the United States, and so we require that governments get a warrant signed off on by a judge that has particular things spelled out that we expect, and here are the reasons we expect to find these things if we execute a search of this person or their home or are looking for a particular document, there has to be that level of granularity and specificity in order for the government to actually gain access to those things, and then use them against you in a court of law when they are going after you, trying to put you in jail, take away your liberty, you know, these are protections for all of us. Justice Kagan, in the majority opinion that was just issued, you know, made the refrain, and this has been common throughout the court's recent cases, that the Fourth Amendment protects the people, it doesn't protect particular, like places, it's for us, it is for everyone in this room to be secure against government's arbitrary authority to interfere and make your lives miserable,

Tim Lordan 08:24
and it's worth noting. Jennifer mentioned I already threw out a few anniversaries, like eight years ago we did Carpenter. Jennifer mentioned 250 years ago this country was born. Basically, also worth noting that the Fourth Amendment was largely comes from the Massachusetts Constitution, which was written by John Adams, who got it from the fact that the British had writs of assistance that just let them rummage through everything, and so he wrote it into the Massachusetts Constitution, which ultimately ended up in our Constitution. And it's worth noting that John Adams died literally 200 years ago today, a few days ago, right? He died on the fourth of July. 200 years ago, on the fourth of July, which is nuts, right? It's crazy anniversary. And Thomas Jefferson died the same day, which is.. I can't wrap my head around that, but worth saying, right? The Fourth Amendment also includes probable cause, and you know, particularly describing the place and the persons and the things, can you like elaborate on maybe Jake or somebody on probable cause and that particularity? So the particularity requirement is meant to basically stop fishing, you need probable cause that what you're searching, that there's evidence of wrongdoing, and that's going to be sought, but you can use that for like a dragnet, so this is going after the kind of the general warrant idea that the Fourth Amendment was largely based on, and kind of in the modern context, that would mean, oh, you know, I have suspicion that, you know, Paul might have committed a bank robbery, that doesn't mean that you can then search every apartment unit in, like, the every unit of the 2000 per.

Jake Laperruque 10:00
An apartment building that Paul lives in, necessarily, you have to actually say, like, well, I think the evidence is in his apartment, or probably more precisely, like in his bedroom. You can't say I want every email he ever wrote over the course of his life. If you are taught, if you're saying we're investigating a

crime that was, we know, was planned in the last week, it's not, it's a way to sort of narrow the parameters of searches to make it reasonable to use the term in it.

Tim Lordan 10:27
In investigators' defense and law enforcement, you know, they're in their defense, in the US v. Carpenter, the Carpenter v. US case from eight years ago, they were actually getting cell phone, I mean, cell phone tower information, and it was spread, the warrant was spread over 127 days. Again, in this case, it was like one hour before and after the crime, right? So much broader period of time, and you know, much bigger geographic distance, you know. And law enforcement would say, well, okay, you struck us down eight years ago with Carpenter, and we narrowed it down. Isn't that enough? Like, would you say that that it's not enough? Because this is a what is a reverse search? What is a reverse search?

Jake Laperruque 11:13
So, a reverse search is a new emerging type of search, searches primarily from technological capabilities that really does flip the whole concept of the Fourth Amendment on its head. The concept of the Fourth Amendment is you need probable cause in particularity that someone committed a crime and you conduct a search based on that. The way a reverse search is, hey, we're going to dig through a bunch of sensitive data and based on that we'll develop a probable cause, who it is. There are a bunch of types of reverse searches, reverse keyword searches, where you say, tell me everyone who Googled this AI prompts, tell me everyone who, or tell me the user who wrote a certain prompt and sent it to Chat GTP, and in this case, a geofence is a location-based reverse prompt, where the government says, hey Google, you have all this geolocation information for your location history, tell me everyone who is in this neighborhood or around this building, or sometimes they're much broader, they say, like, tell me everyone who is in, like, this entire section of a city, and their movements over the course of several hours, or even up to several days, sometimes,

Paula Taske 12:15
and it's, it's worth adding, just briefly, in the context of this, that the court has been very clear that the goal here, when we're, when we're talking about emerging new technology, is to make sure that the same level of security and protection and privacy that was enjoyed by the people at the time the Fourth Amendment was ratified is enjoyed by them today. So, just because this technology exists, just because there's, you know, thermal goggles that could see inside your home, just because there is the ability to track somebody through their phone or their cell phone records. The question is, would that have been reasonable at the time the Fourth Amendment was enacted? And if the answer is no, then you run into Fourth Amendment problems, separate and apart from whether there was an actual search or not. Here, the court found there was a search of the location history, and then the question remains, is it reasonable to conduct that search?

Jennifer Huddleston 13:07
You know, we've talked a lot about the Fourth Amendment so far, but there's another element that really comes into play here, which is this idea of what has been known as the third party doctrine, and I think what most of us on this panel would agree with, or what many people in reading the decision in Chatrie have have seen is what started to be chipped away at in the Carpenter case may not officially be dead

yet, but it's it's pretty much all all but for dead, and in many cases the third party doctrine being a notable kind of exception to some of these expectations, where the idea is, if you know you gave this information to a third party, so again, thinking back to those traditional interactions with a bank teller or a telephone operator, that you have a different expectation in the privacy of that information than you do if you are truly having it in a private setting or something of that nature, and what we've seen is that the court has started to recognize, first with Carpenter, with cell service location information, and now in a broader context, with regards to the Chatri case, that there is a difference in me going and giving Paul a piece of information and knowing that he actually has that information, and me sharing things around general location, or around, or the towers that a cell phone pings off of, that may be sensitive information, but may not have that kind of same knowledge of the sharing.

Tim Lordan 14:34
So, there are a couple of key cases when it comes to third-party doctrine, and by the way, the Washington Post did an editor, the editorial board yesterday, the afternoon did an editorial on this particular issue on this case, and they mentioned the third party doctrine. There's a couple of key cases. Can you maybe Paul like talk about like Miller and Smith, and like Miller was bank records and Smith was like phone records. What were those cases just really quickly about, and like what was the standard? It probable cause to get access to information, or is it lower?

Paula Taske 15:04
Sure, so in those cases one is called the Penn Register case. Basically, this, the officers, you know, attached a device to a phone line to try and, you know, find information about specific phone calls that were happening, and it was argued that there was no expectation of privacy in that sort of information, because you were freely, you know, talking to somebody else on the other end, you know, you weren't really trying to, you know, keep this information secret, and the same with the bank records, you were giving this information freely to a bank, and so by, by making that information, you know, public in a sense, by giving it to another person, there was the argument that you had forfeited any fourth amendment interest in the, in keeping that private, free from government interference, so the government could go directly and say we want this information, and there was basically it was a get out of jail free card for fourth amendment purposes, you know it's been a minute since I looked specifically at the cases to know if they were talking about like whether probable cause was satisfied, but maybe Jake or Jennifer, you remember

Tim Lordan 16:09
well, at least in the Carpenter case they used the Stored Communications Act, which was a much lower threshold to get access to those phone numbers,

Jake Laperruque 16:18
yeah, and I mean the big implications of the third party doctrine for modern society, that sort of the court for decades until now had been kind of dancing around, is okay, so that concept, we, the companies holding these records, that means a third party's access to it, the theory is I don't have an expectation of privacy, I don't have a fourth amendment right, so yeah, the probable cause wouldn't be required because there is no need for a warrant under the third party doctrine that cancels out Fourth Amendment protections of the need for a warrant. Then you get to kind of our modern age and wait a

minute, I have all these documents, like all my work documents and all my personal documents and journals I'm storing on Google Docs, or something else that's held by a third party. My calendar that I keep on my phone is held in the cloud, that's a third party. All my emails and my text messages, literally everything I write on a daily basis, and communicate with people, that's held by a third party. My photo library, it seems pretty just kind of a impossible to stand concept when we look at modern digital life of how, if this idea of sharing for third parties suddenly means no privacy, how does that work in a digital age when our daily lives are built around the idea that things are shared with and maintained by third parties, so that has been kind of, sort of, this looming question for a very, very long time. I mean, we, for over a decade, basically every major email provider has said your emails are provided a warrant protection, they rely on a circuit court opinion on that. Supreme Court has never said your emails are Fourth Amendment protected and entitled to a warrant, that question has just been sort of danced around this whole time, and finally we get to Carpenter, which was about targeted location tracking, and the court finally says, but in a very, very narrow way, well, if it's a cell phone, which are like so tied into daily life that you really don't have a choice to have a cell phone anymore, and they naturally generate these records, then okay, that's not covered by the third party doctrine. It wasn't really a choice to share for third party. That was great for Carpenter, but that's still left with this big question of, well, what constitutes a choice? Is it voluntary to use emails? Is it voluntary to use text message systems? What if I can use a system like Signal, where the third party doesn't have access to the content. What about, yeah, these calendars, cloud storage, photos, documents, on and on and on. It's still really left that question up in the air in a big way, that just we had this looming clash of, well, what happens when digital life meets this, I think, outdated 20th century doctrine. And Chatri seems to have finally sort of stepped in and said, "Okay, we need, we need to resolve this issue. Yeah,

Tim Lordan 19:02
so I, we talked about this before. The panel was, is the, is, is this case Chartres did just eviscerate the third party doctrine, or is the court just chipping away at it, or are they going to.. how do we.. how do we feel about this? I forget how the Washington Post came down on this,

Paula Taske 19:25
I mean, from from my sort of vantage point, I think this is sort of a further cabining of the third party doctrine, sort of elaborating that, you know, yes, we are talking about location data in a similar way that we were, you know, talking about cell phone location information in Carpenter, but we are going to reaffirm that, you know, when we're talking about digital life, the Fourth Amendment still applies to a lot of the analogous, you know, old world things that we would be concerned about in the Fourth Amendment context, things that you would consider to be. Private in the physical world, you can consider to be private in the digital world as well, and so Justice Kagan goes through a litany of those things, and Jake mentioned a few of them: email, your calendar documents that you are uploading, like those things just like you would expect them to be private if you wrote them down on a piece of paper and put them, you know, in a lock box in your nightstand, you can expect them to be private for the digital age as well. So, you know, I think it's helpful, like the third party doctrine is, is relevant, obviously. Still, it hasn't been formally overturned, but I think the court is trying to articulate for for the new age, what we can expect, sort of going forward, how people can expect to conduct their lives in the digital age.

Jake Laperruque 20:50
I think it's, you know, from a legal sense, it is not dead, it is still good law, subject to these two new limits in Chatri. From a practical standpoint, I am kind of happily celebrating the death of the third party doctrine for most digital data and information. I mean, sort of the two broad tests that the court seems to have basically laid out for the future of it is third party doctrine still law still applies unless one the data is really sensitive and two, the user didn't share it for the purpose of the third party being able to use it and share it out themselves. I think it's going to be very hard for any type of important data to not get captured within those tests that sort of nullify out the third party doctrine. I mean, they'll sure be sort of future case law and debates on it, you know, I'd be interested to see, sort of, if the government goes to Amazon or another online retailer and says, I want Jennifer's, you know, purchase records of everything she's bought from you online in the last month. If how you know that would play out in a debate over, does the third-party doctrine still apply there, or you know, if you go to Google and say, I want your Fitbits heart rate monitor to for an investigation. Does that, or other types of health data, meet that sort of two-prong test to say third-party doctrine doesn't apply? There's still not set law on that. I think there's going to be very strong arguments to say, yeah, you're not sharing your Fitbit data because you want Google to be out there talking about your heart rate, and that can be really sensitive information. And then there's a lot of classes where I think it's just it's an open and shut case. No one's going to be able to argue that your email or your online calendar doesn't meet those two standards. Let's get to the second part of

Tim Lordan 22:39
that test sent the sensitive data part right, and how do you know what is sensitive data? I personally think that location data is super sensitive, like I feel like it's like it has also as a creep factor, right? If somebody can know where you're going on the face of the earth at any given moment, that strikes me as pretty sensitive, and and the Energy and Commerce Committee has their Secure Data Act, which is the major privacy bill up here, and it's commercial privacy bill, data privacy, it's not law enforcement privacy, but you know it has four different definitions of sensitive information. One of them is specifically location information, like number four is location information, number one is, you know, data related to race, religion, sex, sexual orientation, citizenship. Number two is biometric information, and third is kids and teens information, and the last one being number four is geolocation information. So, an Energy & Commerce Committee has lumped that, those four together as major classes of sensitive information. Like, can you, Jennifer, can you kind of elaborate on how we look at information, what's sensitive, what's not? Law enforcement says, well, this isn't sensitive information, you gave it to somebody else, why should you have an interest in protecting it?

Jennifer Huddleston 23:53
Yeah, and I think this goes to some of what Jake was saying, it feels like in the location context, in the calendar context, in the email context, this establishes pretty reasonably strong, you know, if you're a tech company of any size, and someone shows up and says, "Give us all this information, you can say, "Where's your warrant? or "Where's your, you know, have you gone through the proper Fourth Amendment procedures and whatnot, v. just a mere request to hand it over. There are also other areas of data where we already have existing privacy laws around how financial records have to be kept around electronic medical medical records under things like HIPAA, where there may be other privacy laws intersecting, particularly in that direct consumer context. Where this is going to be interesting, is in

some of the broader ways we experience some of this data that we may consider sensitive, but how we actually define at what point it is or isn't sensitive. So, think about something like health information. Many people would say someone's health information is something that they would. Consider sensitive information, but to the example Jake just used, it's very different when we're talking about a heart rate tracking app on a fitness device or on your phone v. a medical record. How are things going to play out around those particular types of devices that could be requested in a criminal context, what is going to be the standard there? Similarly, when you think about things like period tracking apps and women's reproductive health, does this provide enough certainty for those who want to make sure that if this is requested by law enforcement agents, that they are able to know those companies know what they can and can't say with regards to what is the expectation of privacy that they can give their consumers, that those consumers know what risks they may be taking in sharing what they may consider to be particularly sensitive information, and then similarly with some of the other elements you mentioned, biometrics, we use biometrics for a lot of things, we may be using them in particular apps, does that then mean that if the requests where you could see almost a concern about a fishing expedition or something. I do think that the Chatrie case, at least, establishes a growing awareness on the Supreme Court around these type of issues, and probably provides a reasonably strong leg to stand on if they were to get some of these requests, should a company want to push back in, in trying to protect their consumers.

Paula Taske 26:28
I'll just add, because I think this is sort of important, as we're talking about Chatrie, the Supreme Court, you know, sort of went back and forth on the government's explanation for why it thought what it did was reasonable, didn't violate the Fourth Amendment, wasn't even a search for purposes of the Fourth Amendment, and they relied on some older cases where the court had blessed certain government actions. One case that they talk about is Knotts, where there was a beeper that was put inside somebody's car to track him as he traveled, you know, from one location to another, and the court at the time blessed that, but they did so in a very cabined way, and Justice Kagan sort of ran through this, saying this was really basic technology at the time, and he was just totally on public roads the whole time for this tracking, but when you went into the next round of cases, where the technology got more sophisticated, more information was available to be tracked, that was when the court was like, no, no, no, there, but no further. When you have things like GPS that can track you, you know, when you're going in public and private, and then obviously the location and cell phone information gives you even more, you know, routine access to people's location in even more discrete intervals, where it's like, oh, the cell phone location data, I think the court said, like, it gives you a ping, like, 104 times a day, and or the cell phone towers do, but the location data is like once every two minutes some new location information is stored about you, and so with each of these new developments, it's like that is a further invasion of privacy, and so I think to Jennifer's sort of analogy, there's a question of like, is the heart rate going to be more analogous to the beeper, or is that going to be viewed along the lines of the location data in Chatrie, where it's like, no, that's super sensitive, where you might think that, like, certainly the, you know, the period tracking that sort of more intimate information would probably fall on the Chatrie line of things, but there are going to be these sort of gray areas where I think either courts are going to have to address them or potentially open the question for legislators to take action, either at the federal or the state level.

Jake Laperruque 28:40
Yeah, and it's worth kind of flagging from that, that the sensitivity of location data is another big aspect of this ruling, kind of the chipping away of the third party doctrines, one, but another reason the government said we actually, this wasn't even a search, we didn't even need a warrant for this, we got our geofence warrant just to be nice, is because Carpenter, back when that happened, 2018 said cell phone tracking in that case it happened for several months. Supreme Court said if it happens for a week or longer, you need a warrant. Definitively, that's the cut off line. Anything less than a week, we'll get back to you later on that. We're not saying it doesn't need a warrant, but we're not saying it does either, and the court, so the government said, well, this geofence, it's only two hours, it's not a big deal, that shouldn't need a warrant. The court pretty definitively said geolocation information, even for any, for any duration, even short durations, is so sensitive and so revealing, especially in a geofence where you can look to the location, you can say, tell me everyone who was at that church or that political rally or that hotel room, when you can go in and get that level of sensitivity. Any type of location information should be held to this level of sensitivity and this warrant standard that gives us a pretty clear path for demanding. Phone data, I'm very interested, like what that might mean for other types of location tracking. So, like, what happens when we have automated license plate readers, which can just, with the push of a button, say everywhere where your car went over the last several months, or track in real time where it's going. What happens if you have a tool like face recognition that can you can take a picture of everyone at a protest, and say, tell me everyone who was at the protest, or stick it outside of a church, or synagogue, or mosque, and tell me everyone who goes in and out of the house of worship. Or what if there's litigation on this right now? What if you have a drone that's constantly flying, you have like a fleet of a few drones that are constantly flying over the city, and you can now use AI tech to tag onto a user and watch them coming out of their house and follow them everywhere they go throughout the day and back and forth, that seems just as invasive as the cell phone tracking. So, I think it's going to be very interesting now that we have this concept on the books of your location information is Fourth Amendment protected, what that means for these other types of powerful location tracking.

Jennifer Huddleston 31:00
If I can just clarify something really quick, I do want to make clear I don't think Chatrie has meant that we have firm answers on those questions yet, but I do think when you see the progress from Carpenter to Chatrie, you are seeing the court more carefully consider these things and not necessarily assume that just because data is shared that that means that in the consumer context, that that means that privacy has been waived in the government context, and you brought up the Secure Data Act, which is more about the consumer data privacy context, and I think that's where oftentimes these conversations either intersect or don't get fully had in tandem, and that they can be separate debates around a consumer may be comfortable giving a company access to certain data for certain use, but not under the assumption that that then means that the government can have access to that same information.

Tim Lordan 31:55
Yeah, can we drill down on that? Like, you know, the corporations and companies collect a lot of information, they have a lot of our information, and but law enforcement can now go directly to them and even purchase those records, like from data brokers. Can we maybe talk about, like, the data broker situation here? And when it comes to the third party doctrine in this particular case,

Jennifer Huddleston 32:16
I think that's one of the concerns is the question of if you are what sometimes you'll hear from folks who are perhaps more proponents of the law enforcement's action in these cases, is well, isn't it better that they at least went and got this reverse search warrant than if they had just gone and bought it from data brokers, and the concern of with that data being out there, are we going to see law enforcement try and use these loopholes to get information that, again, is very broad, is not, is not just about the bad actor or someone with probable cause, can can wrap in a lot of additional information in the particular process. I think it was Paul who mentioned earlier, also around some of these questions that the court didn't necessarily answer, around what is considered sensitive information for Fourth Amendment purposes. How should law enforcement treat digital data? There is a potential for seeing policy that could clearly define any limits on federal law enforcement or at a state level, and we have seen some states, Utah, I know, being one notable example, that have taken steps to clarify at a state level, to ensure that there are what they believe are appropriate safeguards that still can allow law enforcement to access the information that they need when they do have that kind of probable cause, and when digital information can be very important to an investigation, while still preserving civil rights and civil liberties in the process.

Jake Laperruque 33:40
Yeah, I think the data broker loophole and how to deal with that is the sort of big, totally open and unresolved question of this case. Now, I think there's a really good theory to say it should be protected in the same way, because for most of this case we're talking about companies that act as stewards of your data. We don't want Google to be sharing out stuff about your calendar or your emails or your location history. They are meant to hold onto it, and they're providing a service in terms of how they do that. We're talking about with data brokers, is less a steward and more of a sneak, someone who is taking this data without you even knowing it, quite often, certainly without you wanting it to be used in this way, hoarding it, and then selling it off to others. Now, if you, you know, that wasn't really talked about in the case, they talked more about this concept of stewards. Hey, what I'm just using my cell phone, what do I want? Why am I sharing it? But those concepts, I think, certainly apply equally well, for you know, if I have like a weather app on my phone or a flashlight app, and unbeknownst to me, all my location data is being harvested and then sold off to a data broker who's selling it to police or federal law enforcement. Those concepts of you didn't actually intend for it to be shared out and used that way, I think apply. Even more strongly, so there's a good case there to apply it to that, but I think the practical problem that applies is the geofence warrant in Chatrie was issued in 2019 and that geofence warrant is now going back to the Fourth Circuit for further review, at which point we'll see how the Fourth Circuit rules, and then maybe that ruling where there's going to be inevitably a circuit split with the Fifth Circuit, which has said all geofence warrants are unconstitutional because of how broad they are. It's probably going to go back to the Supreme Court. So, maybe like 10 to 12 years after that warrant was issued, we'll finally get a decision on data purchases. We don't have any legislation, even at the start, or litigation even at the starting line, because there's a huge amount of secrecy in terms of how data purchases work when they're used. I don't want to wait 15 years before we actually resolve this question of can the police buy their way around a warrant. This is the area where more than I think anywhere else in this space we need Congress to step in and act, because it's not moving fast enough for the courts to address it in a timely manner

Jennifer Huddleston 36:02
before Paul jumps in, if I can just jump in really quick on the weather app thing, because I think that's a really powerful example of that distinction between expectations around consumer privacy and what we might consider sensitive and expectations around government privacy and what we might consider sensitive, because we all know to use a weather app, the weather app has to know the location you're looking for the weather in, and probably one of those locations is going to be the location that you are using said weather app in. So most people would be reasonably comfortable sharing their location with said weather app, but that changes when it's a should the government be able to know your location just because you opened an app, and I think that can really help us understand why the sensitivity may be different in the government context v. some of the debates where I think there is a concern around how sensitive data can be incredibly useful or things, or if it's defined too broadly, could limit a lot of beneficial things, like location for weather apps. When we're talking about this in the consumer privacy space,

Jake Laperruque 37:09
if I could tack onto that sort of my plea for this is where Congress should step in. Quite often you'll hear kind of when we talk about addressing the data broker loophole and passing legislation to close it. Well, why don't we just fix the entire data ecosystem? Why don't we, you know, we can deal with this as part of consumer privacy legislation. Let's figure out how your data should be bought and sold universally. But I mean, that is Jennifer saying, like, is a really great example of just the equities and the risks in terms of a commercial third party potentially getting access to it, and using it in some ways, and law enforcement are so different. That's really adding, I think, an unnecessary level of hurdles to say we can only tackle the question of, do you want police to be grabbing your location data and buying it all the time? If we figure out how, what are the sort of commercial grounds where we're not going to cut off use of it, like there are just there are practical uses. We probably all want certain safeguards and limits and user controls on it, and the nuances of that have beguiled Congress for over a decade now. Trying to figure out that complex question of what are the right remedies in a commercial sector doesn't need to, and shouldn't restrict us from saying you shouldn't be able to buy your way around getting a warrant in the law enforcement sector.

Tim Lordan 38:27
Yeah, the title of this briefing is legislative includes legislative implications, right? So you know now we have this at least kind of the emergence of a test from the Supreme Court on this particular case, right? Jennifer mentioned a state, the state's kind of taking action. Jake obviously wants Congress to act, as opposed to this case going back and then coming back up to the Supreme Court over a 12 year period, maybe, right, or 15 years or something, maybe. So, talk, maybe, like, would it be better for Congress, the states to step in and start making rules based on does that typically happen after a major case like this?

Paula Taske 39:10
So Congress has responded to various constitutional rulings in the past with separate legislation to address either what they think the court got wrong or if they think the court didn't go far enough in the First Amendment context, the court decided a case in the 90s called Employment Division v. Smith, and really sort of rejiggered how we think of First Amendment religious liberty protections, and essentially

reduced some religious liberty protections, and Congress stepped in immediately, and said, 'Whoa, we do not like this at all. We want the highest level of protection for religious liberty that we can get. We are going to demand that if the government is going to step on religious liberty at the federal level, they have to satisfy strict scrutiny, which. And constitutional law is almost always fatal, in fact, for the government, and so they passed the Religious Freedom Restoration Act shortly thereafter, and that is still on the books today. So, federal, you know, federal law and federal agencies are required to adhere to very strong protections for religion, and so there is room for Congress to act here, you know, to do a lot of the things that Jake and Jennifer have been talking about, to lay out the standards for, you know, some of these open questions, for what does law enforcement have to do in order to, you know, gain access to particular information, where are the red lines here, it's worth noting that they obviously can't pass a law that sets the floor below what the Fourth Amendment would require, but they can always set a higher bar for what the government has to do, and you know, from from my vantage point, just looking at sort of how the Fourth Amendment operates, it's designed to protect us from the government, and so where Congress has a powerful role to play is to set up some of those bright lines to say no, no, we are going to sort of, you know, we're not going to wait for litigation to take its course, but we're going to set the line here of if the government wants this sensitive health information or information from the weather app about certain things they have to do x y and z, and this is going to be the standard that is going to ensure that the people are protected. We are doing this in furtherance of the Fourth Amendment and the guarantees that the Constitution provides. Those sorts of things happen from time to time, and this is an opportunity for Congress and the states, quite frankly, to do something in that, in that regard, too.

Jake Laperruque 41:47
Yeah, there are a couple Fourth Amendment-specific examples. 1960s the Supreme Court passed Katz. This is the seminal decision that says wiretapping, listening on your phone, requires a warrant, is fourth amendment protected, and establishes that reasonable expectation of privacy that really sort of is the foundation of modern Fourth Amendment jurisprudence, and especially for any type of digital information. After that passes, after that becomes law, Congress passes the Wiretap Act and sets out a lot of specific rules and standards for a wiretap that go beyond just a warrant, it creates that super warrant, as we call it, requirement with minimization and all the rules and procedures that really address the fact, like, hey, this is not just a search, this is a really sensitive search, it inherently is grabbing the private communications of people who aren't suspected of a crime, anyone who the suspect calls, so we need to build lots of rules around that. 1970s there was a decision called the Keith decision that was a warrantless search conducted under the auspices of national security. Court said you can't, as a blanket exception, say national security means you get around searches, as far as what the rules should be for that, because national security brings a lot of extra sensitivities. You might not want to go through a standard court. We'll leave it to Congress to figure out the details and bounds of that. Congress responds by passing FISA, the Foreign Intelligence Surveillance Act, creates the FISA court for that process of if you want to conduct national security searches, here's the processes for doing so, and it's a probable cause standard, but it kind of adds some detail to it, that's I think kind of what Congress tends to do best in these cases, is the court usually isn't going to create this like very detailed step by step processes, that's something where legislation is really helpful, that could be for either for geofences or reverse searches, more generally, which is a much bigger and I think much more important question than just geofences, an area where legislation could be really helpful to say,

okay, we have the general parameters, this is a search, I'm sure we'll see kind of as this goes back to the Fourth Circuit, and maybe back up, maybe some overall parameters of how do we limit the fact that you're pulling in a bunch of people that aren't necessarily implicated in a crime, but at its specificity in the form of legislation would be really helpful to have more clear lines and guardrails and privacy rights,

Jennifer Huddleston 44:14
and the only thing I would like to add is typically in the data privacy space we talk about the problems of a state patchwork of privacy legislation, the idea that states acting could create this kind of awful situation where the most restrictive automatically become a federal default, or where consumers and companies have a kind of compliance quagmire, where they never know what the rights or the responsibilities are. When we're talking about this context, it's a little different, but as we're talking about states really restraining their own power and restraining their own law enforcement and creating these additional protections around civil rights and civil liberties, so while it still might vary from state to state what the precise elements of that are, whether it covers all digital data or only certain types of information that the state has decided to. To ensure have these additional protections similar to the the geolocation information in the Chatrie case, it does not necessarily have those same kind of spillover effects, but you're more talking about what should the response be to a law enforcement request, what are those warrant requirements, what are the expectations that that a citizen has around privacy from its government, in that case the state or local government. Instead,

Tim Lordan 45:26
I have a few more questions. We only have a few more minutes, though. But so I want to make sure that we can get to some of your questions. I assume you have some questions, please. But okay, just in the meantime, let me just ask my you guys, think about it. Question, you know, we've been.. we typically, over the summers, do these briefings based on a Supreme Court case, going back like 20 something years. There have been some cases that came out, like, I don't know if anybody remembers the Aereo case from the Supreme Court on copyright, and you just read it, and you're like, I don't think these justices know much about technology. It's pretty, pretty shocking, but you know, after this case, I'm hearing a lot of people, like, you know, dancing in the street, saying these might be the nine most tech savvy member justices in history, right? These people are totally get it. Justice Alito is vibe coding his spare time. Do have we had a sea change in how the court looks at technology now? Is this a new era for the court, or do they still don't really get it?

Jennifer Huddleston 46:37
So I do think they said they were not the nine greatest internet experts, not that they, that they were at one point in a recent case. However, I think what we are actually seeing is perhaps less of a tech savviness and more of a going back to that first principle and recognizing that technology does not change those basic founding American principles, that they're able to take something like the Fourth Amendment or like the First Amendment, and recognize that, as I joked earlier, while the founders might not have understood a smartphone, they understood the principles of what they were trying to do in terms of protecting the people and apply that to the digital age, and there is an awareness that those same principles still apply even when we're talking about the online world or the digital world in a similar way to when we were talking about the mass communications technologies or the privacy questions of the of the founding era.

Paula Taske 47:33
I'll just add that I think the court is certainly learning a lot about technology as technology becomes a much more frequent piece of a lot of the cases that are coming before it, but also you'll notice if you're reading the Chatrie decision, Google submitted an amicus brief in this case to explain a lot of this technology or technological advancements technology to the justices, and Google's brief specifically is cited repeatedly throughout the court's decision, so those sorts of educational opportunities are valuable for the court, just like these sorts of briefings are valuable for folks on the hill, so you know to the extent that anybody's interested in educating courts or legislators in the future, you know that sort of education about new and emerging technology like artificial intelligence, geolocation data is immensely valuable to make sure that the laws and the court decisions that will follow are based on a sound understanding of what is actually at issue.

Jake Laperruque 48:37
Yeah, I think that's exactly right. I mean, there's no way to really know, like, how much of the court getting it is for their own knowledge or through that education with the briefs and work with their clerks and work with outside experts, but I would guess it's the latter, and it certainly seems like they did get it, both in terms of understanding how the tech works and its implications, and also understanding the prevalence of it. There seemed to be like a very good awareness in a way I might not expect with you know older generations of how much this basically permeates every aspect of our society for the average person

Tim Lordan 49:10
I think I had a question in the over here somewhere right there please if you could just stand up and just identify yourself they're great

Speaker 1 49:17
I'm an intern here in the House of Reps for Congressman James from California. I just had a question about kind of that reasonable expectation on privacy, so you referenced Smith and Miller, in which they kind of chipped away at the third party doctrine because those people were freely giving them information. My question, kind of from a younger generation perspective, you know, I have to find my app on my phone, maybe like 12 of my friends constantly have my live locations that they just check out, and I think a lot of people can relate to that, like follow your little things around. So, do you think that there is kind of this warning, especially to young people, or as this. Technology location technology becomes more usable and kind of becomes that norm, but do you think that people are unconsciously forfeiting their own expectation of privacy in their, in within the private sector when they're sharing their location in lifetime 24/7 with multiple people, and is that any different, of course, because this is from, you know, the government v. within the private sector v. new technologies such as Flock cameras that are signing contracts not to people but with city governments in order to collect private data of where you're driving, just etc, etc, kind of different,

Paula Taske 50:40
so in the, in the find my context, if we're talking pre-carpenter and pre-Chat tree, I certainly think there would be a tremendous risk that any sort of sharing of your location data with another person would

have opened you up to a potential, you know, government can just come and find your information in the post carpenter, post chop tree world. I tend to think that the court would view that as a, you know, a targeted sharing with a, you know, a trusted confidant, you know, like you said, you've selected a core group of friends who you are comfortable sharing this with. It's not like, oh, I'm sharing this with the whole wide world, like I'm posting, you know, my live location to my, you know, YouTube channel or my Facebook, and so anybody who can view my profile could see my live location in the very moment there. I think the court might very well say, "Well, you forfeited any sort of expectation of privacy there, but in, in so far as it's shared on your phone with another person that is trusted by you. Maybe this is optimistic of me, but I tend to think the court would be less inclined to say you forfeited the privacy interest there. The flock cameras are a little bit interesting. Just define

Tim Lordan 51:52
what a flock camera flock camera is.

Paula Taske 51:54
Yeah, so the flock cameras are basically cameras that are posted around the city that can take images of you in real time, you know. I think it might depend, but I think there's probably less of a Fourth Amendment expectation of privacy there, because it's, it is a public image of you that can be taken at any point. I mean, I think the court has even still been fairly consistent that, like, if you are in plain view in public, you know, snapping a picture of you is, you know, not necessarily a violation of your privacy. They sort of have tried to balance the line of, like, if it's constant surveillance that will raise Fourth Amendment concerns, but you know, a standalone image, like a traffic camera, similar to Flock, might not raise Fourth Amendment issues from the court's perspective.

Jennifer Huddleston 52:41
So, I think there's going to be a lot of distinctions there. I mean, I mean, I disagree with Paul, in part because it's going to, of course, with something like the flock camera depend on on a number of issues, including, you know, we talked a bit about some of what's going on with automated license plate readers, and is this something that's becoming used as a form of surveillance, or as a way of perhaps limiting other rights as well. Is this something that's being used to, or the flock cameras being used to take a picture of a protest that's then being used to silence First Amendment rights, and in the process as well. So, I don't think it's as clear cut as just a you are in a public place and someone takes a picture of you in that particular context, and this goes to part of the kind of concern that arose recently when there was a conversation about Amazon Ring potentially partnering with Flock to help find lost dogs. Finding lost dogs is good, I'm a cat owner, but finding lost dogs is good, but a lot of people had concerns about how this would open up all of private individuals' ring cameras to be monitored by law enforcement, potentially at all times. To your original question, though, about fine mind, I think this goes back to we all perhaps need to think through our privacy preferences carefully, and we also need to recognize that for most of us, while privacy is a value, we are going to make choices where we choose other things over privacy, whether it's that you feel safer because so many of your friends or your mom or whoever has your location, recognizing that that may erode a little bit of your privacy, and that you're having to share that with the company who gives it to them, but that's a very different private decision with regards to your privacy than the context here, where we're talking about, does your decision to waive some element of personal privacy preference for the select group also waive it for the

government, and I think that's where that distinction, and where we start to see clarity from Shahri in the geolocation situation, but where we could see further clarity as this type of context comes up in other environments as well, ma'am, I had a question. I don't know if you

Jake Laperruque 55:01
wanted to. I'll just quickly say, I think what folks who grew up with phones and social media kind of inherently recognize, and that the court's starting to get a hold of, is that privacy today is not a binary, it's not just simply the private sphere and the public sphere. There are kind of like I call it sometimes like onion privacy, it's like there are layers of privacy, where I mean, just because you share your location with a couple friends you want to see, make sure you get home safely from, like, the bar after a date, doesn't mean you're going to privately share that with everyone in your address book, and certainly doesn't mean you're going to share that with the FBI, and then you know that's true of all kinds of information, yeah, just because we kind of might share if a company, hey, hold on to this data for me. Oh, use this data to help me find this website I'm looking for a recommendation for a website. It's not an all or nothing proposition. So, I think that that's how people look at privacy by and large, and that's kind of what the law is adjusting to.

Speaker 2 56:00
Hi, my name is Sophie. I'm a lawyer with EqualAI. We're a nonprofit organization that focuses on AI governance. My question is, I mean, this has been such a fascinating briefing. There's a lot of distinction on, obviously, with the Fourth Amendment, like what in third party doctrine, what does the government have access to v. private organizations, and I keep thinking, like, does the distinction matter that much when the type of companies that have access to all of their personal information are the wealthiest companies in the entire world and have consolidated extraordinary amounts of wealth and power in ways that earlier questions about third party haven't necessarily been brought to the Supreme Court, I'm not sure you know the reliance on Apple is comparable to other systems that have been able to track local information, so I'm curious, how the size of somebody's big tech and like the overwhelming role it kind of plays underlies some of this conversation, and also how we're thinking about what is the consumer's responsibility to behave and consider privacy?

Tim Lordan 57:12
That's a lot to answer in the 60 seconds we have before the hard stop.

Paula Taske 57:17
I'll just quick, I'll try to quickly answer by getting some of the clues that maybe we have from Chatrie, and it's sort of in the introduction when Justice Kagan is talking, she's talking about the prevalence of cell phones, how important they are, the fact that so many people have them, obviously the cell phones are made and distributed by some of these large companies that have a lot of this, you know, money and are creating this technology, and you know that feeds into the court's approach in terms of whether it's reasonable to expect some of these things to remain private, and I think we're going to see that in the AI space sort of develop, maybe you know, over time as the court wrestles with this, but I think it will be similar as AI adopts a similar level of prominence and prevalence in daily life to what we're seeing the court sort of move to in terms of cell phones and other digital technology. I

Jennifer Huddleston 58:08
am going to do that annoying thing where I'm going to somewhat answer the question that I want to answer out of that question, rather than the question that was actually asked, because I think one of the underappreciated elements of these kind of rulings is what they mean for smaller tech players. If you're a large player and law enforcement shows up, that's one type of threat, but you also probably have an army of lawyers at your disposal to help you navigate what are the nuances. Is this covered by Chartres? Can we fight this? Can we ask for more information, et cetera, et cetera. If you're a two-person startup and suddenly law enforcement knocks on your door with a request that can be a very different situation, and so I think one of the good things that we are seeing is how this provides more information, so that all companies can have the appropriate response to protect their consumers from potential government intrusion.

Jake Laperruque 58:57
Yeah, I'll say kind of two reactions on it. First, I do think there are some unique aspects of why government surveillance is dangerous and why it should be held to an especially high standard. No matter how big and powerful Google, Meta, Amazon, whoever else is, or the government can arrest you or detain you and deport you, or have a bunch of armed agents bust into your house and potentially shoot you. Those are powers and levels of force that we reserve to the state, and that means the state needs to be checked with things like the Fourth Amendment in unique ways. That said, yeah, I mean, it's certainly it is an area that is really important, and even if they can't arrest you, that's a lot of power that is not properly limited, so I'll not only caveat that for my first remark, but also what I was saying earlier about, hey, don't let consumer privacy get in the way of making passing something like the Fourth Amendment's Not for Sale Act and cutting off the data broker loophole for law enforcement. Yeah, I don't think those need to be solved all in one go, and you have to. Wait for one to do the other, but passing comprehensive consumer privacy legislation is really, really important, and is not exactly the same set of threats that we are taking on here in terms of government surveillance, but it is also really important for your privacy in an area where there are a lot of needed safeguards that just aren't there right now.

Tim Lordan 1:00:21
I am truly astounded that we got through 59 minutes without mentioning artificial intelligence. That's like really rare in this space, and also it's worth saying that we didn't get to it. I think we were going to, is like after poor mr. Chatrie was arrested, Google had actually changed its procedure, so that type of warrant wouldn't have been possible, so that's another. We didn't get to that, but that there's elements there too. I promised Paul a hard stop at one, because he has to exit. Started left for a meeting, and I want to thank the caucus co-chairs for hosting, and everybody for coming. Thank you, everybody. Thank you.

1:00:56
Thanks, Paul. Sorry, I.