Chatrie and the Future of the Fourth Amendment

Thursday, August 27, 2026

Visit our media library at constitutioncenter.org/medialibrary to see a list of resources mentioned throughout this program, listen to the episode, and more.

[00:00:00.2] Julie Silverbrook: From the National Constitution Center in Philadelphia, this is We The People.

[music]

[00:00:07.8] Julie Silverbrook: I'm Julie Silverbrook, Chief Content and Learning Officer. The National Constitution Center is a nonpartisan nonprofit chartered by Congress to increase awareness and understanding of the Constitution among the American people. In a recent decision, the US Supreme Court held that law enforcement's use of a geofence warrant, which collects identity and location data from mobile phone users, violated the Fourth Amendment's protection against unreasonable searches and seizures. In this episode, we unpack the decision in *Chatrie v. United States* and discuss what it means for the future of the Fourth Amendment, privacy, and government surveillance in the digital age. To help us explore this, we are joined by one of the nation's leading scholars of the Fourth Amendment and digital privacy. Orin Kerr is the Stella W. and Ira Lillick Professor at Stanford Law School and Senior Fellow at the Hoover Institution. His most recent book is, *The Digital Fourth Amendment: Privacy and Policing in Our Online World*. I'm very excited to share that Orin will also be the lead faculty in the Center's new online Fourth Amendment mini-course, which will launch later this year. Orin, welcome back to We The People.

[00:01:11.8] Orin Kerr: Julie, great to be back with you.

[00:01:14.0] Julie Silverbrook: Orin, you've called *Chatrie* a blockbuster and the most important Supreme Court decision on the Fourth Amendment and new technology today. Why is this case such a big deal and yet so few people are paying attention to it? Or as I like to say, why is no one chatting about *Chatrie*?

[00:01:32.4] Orin Kerr: So it's a big deal because it really recasts what Fourth Amendment privacy is about, and it adopts a bunch of new ideas that suggest a very broad set of Fourth Amendment protections in the new internet world we're in. So one of the big issues had always been how do you apply the Fourth Amendment to a network world where you are inherently disclosing your records, your information, your data to third-party companies, to other people out in the world? I mean, what you're doing when you're using computers is you're sending

communications out into these networks. And a big question had been how do you apply this Fourth Amendment protection, which is really about protecting your home, to this new world where you're sending all this data out? And the Supreme Court's answer is basically, we treat all that data sent out as if it's in your home. We extend broad protection over all of these records that you're using from your phone. And that is a surprising decision that is gonna... That suggests very broad Fourth Amendment protection. As for why people are not paying attention to this, I wish I knew. I think probably because there's nothing directly related to Donald Trump involving this, and everybody wants to talk about presidential power and Donald Trump. And this is kind of a traditional Fourth Amendment case that 10 years ago, 15 years ago would have gotten a lot of attention, but at least right now has not received the attention it deserves.

[00:03:02.3] Julie Silverbrook: I think it's most likely going to end up being a hugely consequential case. So I really wanna get into the details, and let's start with the facts. What is a geofence warrant? And how did the warrant used after a 2019 Virginia bank robbery ultimately lead investigators to Okello Chatrie?

[00:03:23.5] Orin Kerr: A geofence warrant is a warrant that goes to an internet company, some big provider here. It was Google and says, tell us the locations of phones that were in a particular geographic area at a particular time. And so the government, for a window of time, was using this quite often as a way of figuring out who committed crimes when the government knew a crime was committed at a particular place at a particular time, but they didn't have suspects. So it's a cold case. They know somebody was beaten up or a bank was robbed in the case of *Chatrie*, or someone was assaulted, whatever it might be. They know where, they know when. They just don't know who. And so the idea of geofence warrants is to find out whose phones were in a particular area at a particular time to create a list of suspects the government can look into. And this was used in the *Chatrie* case to solve a bank robbery. Government knew the bank was robbed. They knew where the bank was. They knew when the bank was robbed. They just didn't know who was the robber. And it turns out Chatrie is one of the people whose phones were turned on and had logged into Google and had this feature called Location History turned on. And that enabled the government... It was basically, Chatrie kind of turned on a tracking feature and then robbed a bank, and the government was able to find out he was there at the scene of the crime because he had turned on this tracking feature. And the question was whether the government needed a warrant in order to get these records or whether they were outside the Fourth Amendment entirely. And that was the search question, is the one question that the Supreme Court answers.

[00:05:04.4] Julie Silverbrook: To understand *Chatrie*, we need to go back to a 2018 case, *Carpenter v. United States*. What did *Carpenter* hold about cell site location information, and how did it qualify the traditional Fourth Amendment rule that information that's voluntarily disclosed to a third party, like Google, generally loses constitutional protection?

[00:05:26.3] Orin Kerr: Great. So the background rule before this 2018 decision, *Carpenter*, that you mentioned is that when you knowingly disclose information to someone else or something else, you give up information in what you disclose. So if you and I meet and I tell you I robbed a bank last week, and the government comes to you and says, "What did Kerr tell you?" You can say, "Kerr said he robbed a bank last week." And I don't have any Fourth Amendment rights in that because I told it to you. You are kind of an eyewitness to what I said. And before the 2018 decision, *Carpenter*, the Supreme Court had applied that principle pretty broadly. So, for example, the numbers dialed, when I dial a telephone number, I'm telling the phone company, "Here's the number I'd like you to connect me to." And the government could then go to the phone company and say what number was dialed. And so the Supreme Court said that's not protected under this idea called the third-party doctrine. The information was voluntarily disclosed to a third party. In 2018, in *Carpenter v. United States*, the court puts a limit on that. They say this disclosure idea is not an automatic rule. Rather, it's sort of a matter of degrees. And if the information was extra private that was disclosed, then maybe the disclosure doesn't eliminate all privacy in that. And that also there's kind of a baseline amount of disclosure which, living in a modern society, we have to permit. So the 2018 case involves cell site location information.

[00:06:53.4] Orin Kerr: Those are the records generated by your cell phone whenever it's turned on and connected to a network. You'll notice when you turn on your phone, you'll get five bars, for example, showing you have a good connection. That's showing you have a strong connection between your phone and a local cell site. That is a network connector that the phone company has that allows the communications to be delivered to your phone and sent from your phone. And so when you turn your cell phone on, it's not just magically working, it's connecting to a local site. And that created effectively a way of determining where people were to a very rough extent, sort of within maybe a half a mile based on where their phones were. So, for example, if the government knows where my... Knows my phone number, they could go to my phone provider and say, "Give me the rough area where Kerr's phone was located." And probably I'm with my phone. And by knowing where my phone... Which towers my phone had connected to, you could sort of get a rough idea as to where I was, what town I was in, for example, not what room, but what sort of neighborhood. And so in the *Carpenter* case, the government had collected records of the cell site location information of Carpenter, who was involved in a series of thefts of cell phones, ironically. And they showed, oh look, wherever there was another robbery of this store, Carpenter's phone happened to be in the general area, suggesting that he was involved in the crime. And the Supreme Court said that's not a case of third party disclosure because this information, location information is very sensitive first. And then also you have to kind of consider the baseline amount of privacy that people have. You need to carry a cell phone to participate in modern life. And so you're not really voluntarily disclosing records to the phone company. You're just kind of doing what you do in life, which is carry a cell phone. And so that's not a voluntary disclosure. Putting a limit on this idea of third party disclosure, which then the *Chatrie* case returns to and very much expands on that idea.

[00:08:58.2] Julie Silverbrook: Well, let's talk about that. Because when you turn on your cell phone and you download an app, you're often prompted as to whether or not you want those apps to track your location history. So unlike in some ways the cell tower, right, to use your cell phone you have to do this, in most instances actually you don't have to have location history turned on to use apps. You can opt out. And yet Justice Kagan, in the majority opinion applying *Carpenter*, I think goes even further than *Carpenter* did.

[00:09:35.0] Orin Kerr: It definitely goes further than *Carpenter* did. So *Carpenter* says, well, this is a unique case of records you can't avoid. And then *Chatrie* then says, well, it's part of using a phone. It's kind of ordinary phone use, and therefore this third-party doctrine doesn't apply. So the big difference here, as you pointed out, is you don't have to log into these services. And in fact, there's a series of steps to have location history turned on and working. You needed to not only have a Google account, which most people do, but sign up for this location history, turn on location history on the phone being tracked, and keep it on. Now you didn't... If you turned it off, it would stop working. And I should also point out this was a technology that existed that Google changed. So now Google doesn't have these records anymore. They can't do this geofence warrant anymore. So this was up to a period of time this technology existed. But the government's argument was, well, wait a minute, you don't need this. This is optional. This is something that you can opt into and that Chatrie turned on the tracking device. Right? It's like, "Would you like us to track you?" "Yes, I would." And then, well, how can you voluntarily say, "I want to be tracked," and then object to the tracking essentially, or object to the government collecting the tracking? And so the Supreme Court's answer to this is you have to consider not what's required to participate in modern life, but rather the kind of category of ordinary cell phone usage.

[00:11:04.0] Orin Kerr: Sort of anything that counts as conventional or ordinary cell phone usage, that is exempt from this disclosure rule, and therefore the fact that somebody turns it on doesn't make a difference. And I should say this was something that was actually quite hard in the record in this case. So the idea of opting into this, the government said, well, most people don't opt in. And my own kind of independent research suggested actually geofence warrants rarely work because most people didn't log in, and so the government could never find the person who committed the crime. They just, they didn't opt into the tracking, or they didn't have their phone on, or whatever it was. It actually rarely seems to have worked. But the government's argument is like, you've decided to... You've opted into this. And from a record standpoint, what makes it hard is that exactly what a user encountered actually was not fixed. So it turns out iPhone users and Android users had different screens, different sort of opt-in procedures. And it's like, you get a screen that has a lot of text and then there's a little bit of writing at the bottom. Do you consider that writing at the bottom the message that was sent about whether you have to opt in? So some of the language was like, "If you don't do this, your phone won't work properly." And the court's answer to this is to say effectively what Google was doing was pressuring people to opt in. You kind of had to, or at least, gosh, you'd feel pretty

pressured to do it. And I think that was a little bit of a creative reading of the record, but that's at least the court's way of construing the record.

[00:12:38.3] Julie Silverbrook: I sort of was just thinking about whether or not the average person looks at the language, right? You download the app, you kind of wanna get to using it, and so most people don't even read the opt-in, opt-out language. And I do think the default in a lot of cases, if you don't select to opt out, you're opted in. Right? Like it's not a "I'm choosing to opt in or out." The default is you opt in unless you read through and then select opt out. And I did wonder if just because sort of the reasonableness of this, right, sort of the average person, right, would assume that they've maybe not opted in to that kind of tracking.

[00:13:20.5] Orin Kerr: Yeah. So I call this, in my paper on *Chatrie*, I call this the black box problem, which is to what extent do you assume people understand the technology they're using? So a lot of times the nature of a technology is like, it's doing a certain thing, and you might have a novice user who doesn't understand what's happening. It's just kind of like a magic black box that just, it just works and you don't know what's going on, versus a user who's like, "Oh, yeah, when I dial a phone number, for example, am I giving the number to the phone company such that the phone company now has the number, or is it just like a magic thing? I enter in the numbers and like, boom, a connection has been created in the universe." And so there's this underlying question of to what extent do you think of this as like, well, we assume the user understands what's going on, or we assume the user doesn't understand what's going on? And a lot of times you get a really different kind of assessment of what's happening technologically, just in terms of the facts, depending on which assumption you make.

[00:14:21.5] Julie Silverbrook: So after *Jones* and *Carpenter*, the court has wrestled with what you call the mosaic theory. It's the idea that surveillance that is not initially a search might become one once enough information is collected. What does *Chatrie* do to that theory, and why does that matter for Fourth Amendment law?

[00:14:39.2] Orin Kerr: Yeah, *Chatrie* does two different things, and it's worth separating them out. So the first thing the court does is say there is no accumulation theory, that if you do enough of the thing, eventually you cross a line into a search. And so this is a recurring dynamic in technology cases where a lot of times technology allows the government to do something a lot of times. They can track someone a lot. They can watch somebody for a long time. They can... Computers are amazing at just doing the one thing over and over and over again. And so some courts had said, well, that suggests that you should be... The government should be allowed to do a little bit of it, a little bit of surveillance, but then not a lot of surveillance. And how do you draw the line between the old tech and the new tech effectively? The Supreme Court's answer is you can't draw a distinction between accumulating a little bit of records versus a lot of records. There's just no line to draw there. And a lot of times getting a few records but very sensitive records is more invasive than getting a lot of records that don't actually show very much. So

we're not gonna draw a distinction between like short-term surveillance and long-term surveillance, or one record versus 100 records or a million records. On the other hand, the court says we are gonna draw a distinction between kind of technologies that are capable of doing mass surveillance and technologies that are not capable, or are or not.

[00:16:01.1] Orin Kerr: And so they distinguish this 1980s case on a radio beeper, this case called *Knotts* from the early 1980s, and that was tracking a car around town with a radio beeper in the car that allowed the government to kind of, as long as they were relatively nearby, they could know exactly where the car was because there was this little surveillance device that was inside the car. And so in the 1980s, the court had said, well, you have no reasonable expectation of privacy in public on a public road, and therefore that's not a Fourth Amendment search to track someone who's had this radio beeper installed. But then the court had suggested, actually, it's different if it's GPS surveillance and the government's able to track a lot. And the court says, "Okay, the line here is not over time it starts to become a search, but rather the inherent nature of the more advanced technology is to allow greater scales of searching." So we will allow basically rudimentary surveillance tracking without it, that won't count as a search, but if it's a technological tool or service that has the capability of broad-scale monitoring, like these more advanced technological tools, then those things will be considered a search even if it's just one piece of data that's collected.

[00:17:20.6] Julie Silverbrook: Talk a little bit about the court's emphasis on whether users understand information stored by a company as still being their own and that impacting the analysis about whether or not there's a reasonable expectation of privacy?

[00:17:36.9] Orin Kerr: Yeah, so this is an issue in the case which was to what extent, when... Should it matter when you're talking about the privacy implications of the record, how do you determine what is a private record, becomes a very hard question. What information is private versus not private? Because a lot of information in context, it might actually be pretty private. Depending on what else somebody knows, a lot of information can be considered private, or depending on the context, not so private. This is something that courts have really grappled with. One of the approaches the court takes in *Chatrie* is to suggest that the user's perception that the record is effectively their own makes the record more private. So this is a difference between *Carpenter*, the cell-site location information case, and *Chatrie*, the location history case. In *Carpenter*, most people don't even know these records exist. So most people have no idea that their phones are generating these cell-site location records. And so they're just kind of business records that are out there. The court in *Carpenter* said those are still private records. But in *Chatrie*, the court says, "Well, with location history, it's even more private because the user's looking on their phone, on their app, and they're seeing these records. They kind of think of them as your own records." It's again this kind of ordinary user perception of what the kind of regular person who doesn't have any idea where those records are stored, what do they think of the records? And it's especially interesting because those records used to be ones that were stored

with Google, that when you'd look on your phone, if you opted in and all that, you'd look at those records and they would be coming from a server at Google. Now those are coming from inside your phone. So now those actually are your records inside your device. But most users would not have any idea that that was going on, especially at the time.

[00:19:28.1] Julie Silverbrook: I was also thinking about the differences between *Chatrie* and *Carpenter*, and the cell tower data is not as precise, right? So they were able, with the Google location history, you can get to a few feet away from, in this case, the bank that they were looking at, and they were able to really narrow down who was there because of that. And I did... I'm curious if the precision of the information matters?

[00:19:59.0] Orin Kerr: It does. It does on this initial question of whether the records are one that are protected by a reasonable expectation of privacy. The... At least the, court's first step is to say, "Well, we decided *Carpenter*, and we looked at the kinds of records that existed in *Carpenter*, and now we look at location history, and these are also precise location records." In fact, they're even more precise than the location records in *Carpenter*, as you suggest. Now, it's a little bit of a funny connection or comparison because in *Carpenter*, the court had said, "Well, these records aren't very precise, but the technology is moving in a direction of being extremely precise, so we have to kind of take where the technology is going as our standard." And I think actually the technology turns out eight years later hasn't actually changed, but that's at least the court's prediction. In *Chatrie*, the court says, "Well, this is now super precise. So these are really private records." And it's this idea that the court is to look at the nature of the records collected and kind of assess the degree of privacy inherent in the abstract in that record, which is an idea that becomes a little bit hard. The traditional way of thinking about the Fourth Amendment is that there's, where is the record that matters, sort of.

[00:21:16.6] Orin Kerr: If the government breaks into your house, they need a warrant 'cause entering your house is a search. It doesn't matter if they only read the newspaper on your kitchen table, it's still entry into your private space. And if you wanna go out into a public park and talk about your private things and the government is standing there and they overhear you, the fact that it's really private information doesn't matter because you talked about it in public. So the traditional Fourth Amendment answer is like, "We can't evaluate what's private and non-private information. We can only evaluate like where is the information." And we're gonna focus on the location. Now it's actually the court assessing the degree of privacy inherent in that category of information to then determine whether a warrant is needed to get that information. And we're in a technological world where internet providers, cell phone providers, they have lots of different kinds of records. So the big question going forward, or one of the big questions is, well, what do we do with the amount? How do we assess the privacy interest in all that other information that these providers have? Is it all private? Is the court's gonna go through and kind of categorize different kinds of information and say some of it's private, some's not? And lower courts are just gonna have to grapple with that for the time being.

[00:22:31.5] Julie Silverbrook: It's so complicated because your papers and effects are all in your phone basically, right, or on your computer, and that often travels with you. It feels to me there's gonna be a lot to grapple with to kind of figure out where to draw the line, right?

[00:22:49.0] Orin Kerr: Maybe. And actually I should clarify that the items that are actually on your device, so they're on your phone, those are pretty clearly protected. So going back to 2014 and *Riley v. California*, the Supreme Court says the government ordinarily needs a warrant to search your actual phone. What we're dealing with here is what about all these third-party stored records? The... You log into an account, social media account, and the social media company is keeping records of which account logged in, when it logged in, what IP address it logged in from, what it's doing. And a lot of times these companies keep very comprehensive records about what kind of is going on there. Well, does that mean all those records are now protected? If the government wants to find out when someone logged in, what IP address they logged into, whether an account even exists, that also could be something just to verify if an account exists. Does the government need a warrant now for all of those things or only some of those things? And we just don't know at this point.

[00:23:50.3] Julie Silverbrook: This was also an unusual lineup. Justice Kagan wrote for the Chief Justice and Justices Sotomayor, Kavanaugh, and Jackson. Justice Gorsuch concurred in the judgment, and Justices Alito, Thomas, and Barrett dissented. What are the most important differences among those approaches articulated in their opinions, particularly Justice Gorsuch's rejection of the *Katz* reasonable expectation of privacy approach in favor of a more property-based theory?

[00:24:17.8] Orin Kerr: So Justice Gorsuch's opinion was pretty predictable based on his approach in *Carpenter*, where in *Carpenter* he'd said, "I think this *Katz* expectation of privacy idea is made up. We should go back to the traditional Fourth Amendment approach and follow the text of the Fourth Amendment." And the problem is you kind of end up recreating the same conceptual questions, I think, whether you go with expectations of privacy or searches of persons, houses, papers, and effects. A lot of times you end up kind of asking the same question. To my mind, that suggests they should probably just adopt some sort of consensus textual and privacy-based approach, but they have not done this. Instead, you get the majority by Justice Kagan really strongly embracing privacy, a privacy approach to the Fourth Amendment, not concerned with the text of the Fourth Amendment as much, not concerned with the history as much. Instead, it's a very broad conceptual privacy approach.

[00:25:12.7] Orin Kerr: And then Justice Gorsuch, following up his *Carpenter* opinion, his separate *Carpenter* opinion, whereas in *Carpenter* he said, there are a bunch of hard principles here, I'm not sure what we should do, we should think more about this. In his *Chatrie* opinion, he takes a view and says it's a search to collect the location history records because those records are effects of a person. So the fact that Google has the record of where the person is, but those

records are a person's effects. And he looks primarily to the terms of service that Google has and also the existence of state computer crime laws that say, here we're gonna protect records that are held by a computer, and sometimes they call them property. And so he basically says there's enough here such that the records are effects. Gathering those records is seize, it should be really seizing, but searching those effects, looking through them. And so Justice Gorsuch gets to the same result through what's really, I think, a textualist property approach, but it requires a theory of what counts as effects, which is pretty novel to the *Chatrie* opinion that he writes.

[00:26:22.6] Julie Silverbrook: Let's get into the dissent a little bit as well, Justice Alito's opinion.

[00:26:28.1] Orin Kerr: So Justice Alito's opinion proceeds on a couple of different grounds. First, he's annoyed that the court is here at all. He's annoyed that the court... Annoyance is the wrong word. He thinks that the court should never have taken the case, that what makes this case unusual, this was a very unlikely cert grant from those of us who were watching this. I was aware that there was a petition for certiorari filed, but I was like, yeah, sure, whatever, that total Hail Mary pass, no way they're gonna take that, because everyone knows that the good faith exception to the exclusionary rule is going to apply. The idea of the good faith exception to the exclusionary rule is that a criminal defendant should only be able to get evidence suppressed, that is, thrown out of court, if there's a pretty serious violation of the Fourth Amendment. Not every violation counts. It has to be a major violation. And so what counts as a major violation that justifies suppression of the evidence versus a minor violation that doesn't is this really hard issue which gets sort of covered under the rubric of the good faith exception. It's a bad label because it's not really about someone's subjective good faith. Instead, it's about these complicated rules about what counts as a minor violation and a major violation.

[00:27:41.5] Orin Kerr: In a 1984 case called *United States v. Leon*, the court had held when the government gets a warrant, the good faith exception applies to defective warrants unless it's a really blatant violation. Officers should have known this warrant is defective, there's no probable cause, there's insufficient particularity. And what this means is if you're a criminal defense lawyer and the government got a warrant to search your client's house, for example, unless it's an egregiously bad warrant, you're not gonna get suppression of the evidence even if you look at the warrant and you say, this is actually... This violates the Fourth Amendment, they did something wrong here. So it has to be an egregious violation. Well, you can't really get to an egregious violation when you're dealing with a technology, it's not clear that a warrant is needed at all. The government got a warrant. There are a lot of theories as to why this was a perfectly plausible warrant. It might have been constitutional. In fact, the court doesn't address, the Supreme Court doesn't address whether it was a defective warrant or not. They leave that, they send the case back to the lower courts and say, you guys figure that out. And so in the end, it's reasonable that they obtained this warrant they obtained. They have no idea how the Fourth Amendment is going to be deemed to apply years later.

[00:28:54.3] Orin Kerr: And so it's pretty clear there's not a remedy and that this whole case is really just about announcing rules prospectively for kind of going forward, here's how the Fourth Amendment applies. And there's a live dispute in the sense that there's a formal case pending, but it's just sort of understood that no matter how the Court rules on what's a search or what's a reasonable search, the good faith exception to the exclusionary rule is going to apply, and so Chatrie is never gonna actually get relief no matter how the Courts rule. And Justice Alito thought the Court should never have taken the case. His broader concern is he's basically saying, "Well, wait a minute. The Fourth Amendment as originally understood was about physical entry into the home, was about physical intrusion. Then we expanded it to non-physical intrusion, and then we expanded it to things, or deeming things involuntary in order to protect sort of cell-site location information. And now it seems like we're kind of protecting everything out in the world." And his concern is, what's the limiting principle on this? How far... We're just sort of taking, "Oh, privacy. There's sort of private things out there. We should all protect private things." And that's not traditionally what the Fourth Amendment was about in the abstract, and now the Court is really embracing that. And the Court does, in the majority opinion, they really embrace at a rhetorical level this incredibly broad, Fourth Amendment protects any unjustified intrusion on the privacy of the individual of whatever form. And that's honest language. That's a really free-form sort of idea. And Justice Alito is basically saying, "What are we doing? Why... This is a voluntary step and we've never construed anything this broadly. Why are we extending the Fourth Amendment to these new facts in this sort of very vague privacy idea? And this would seem to protect everything in a digital world, and we shouldn't be doing that." is basically the idea.

[00:30:47.1] Julie Silverbrook: Well, I think it's a great question, and you start talking about this question in your latest paper. And so I wanna get into how you're reading *Chatrie* now that the decision is out in the world. So in your latest paper, you identify basically three possible ways to read the case. You can read it as a case about location records, you can read about a case about cell phone records, or most broadly as a case about third-party records held by technology companies. Walk us through those three readings and what the implication would be of all of them?

[00:31:21.6] Orin Kerr: Yeah, so the narrowest reading of *Chatrie* is that it's really about location records. So all of these cases, *Carpenter*, *Chatrie*, are about a specific type of record. It's a record about where somebody was. And so one way of thinking about these cases and *Chatrie* in particular is to say what the Court's really worried about is we've entered a world in which tracking people is easy, and we don't want the government to have this sudden ability to track everyone or to track a lot of people because of the sort of happenstance of cell phones. And so you have a reasonable expectation of privacy in your location, and location is special, and the case is not really necessarily connected to all the other records, and there are all these other cases of different kinds of technologies, and that's sort of a separate issue. And if that's the reading, you'd say, "Well, location records are super sensitive and the courts should be focused on

technologies that reveal location." And that actually raises some hard issues of what does it mean for a record to reveal location? Because all records to some extent reveal location. Going back to the 19... The early case of numbers dialed from a telephone, well, that was a landline phone, so the fact that a number was dialed from that phone gave you location records, the caller was in the home. It wasn't what it was about, but you can sort of imply that there are these facts.

[00:32:51.1] Orin Kerr: And so what counts as a location record is pretty hard, but one reading of *Chatrie* is it's really about the special concerns about big brother tracking and making sure that the government needs to get a warrant for that kind of tracking. Next reading of it is that this is really a case about cell phones, that cell phones have just dramatically shifted what's private and what's not private. And it's led to a world in which cell phone users are constantly communicating with these internet companies that store our data. And we need to make sure that that data is protected because otherwise basically everything you're doing all day is left exposed and the government can just go to these internet providers. And so we need to kind of have special rules for cell phones because of how cell phones work. And one issue that raises is, well, why cell phones? What's different between a cell phone and any other thing? Because cell phones are really just computers that happen to be handheld, that have a network capacity, that sort of have... They connect to local cell towers. But that's like the connectivity, that's not what the devices do. And so why would cell phones be different? Is it gonna be a rule that if you dial a number from your cell phone, the government needs a warrant to get that, but if you dial it from a landline, the government doesn't need a warrant for that? Like sort of a weird sort of tech tool-by-tool approach. Maybe that's what the Court's doing, but we don't know. And then the last reading is that *Chatrie* is... This is the broadest one. This is just about third-party records generally. And what the Court is doing is saying, "Listen, we're moving into an internet world where so much of our life is mediated through these major companies that have all of our records. And we're just gonna say all of that is protected.

[00:34:37.2] Orin Kerr: The government needs a warrant to get any of it." So the government gets a windfall in that records exist that wouldn't exist of what people did in the past. But in order to get access to those, the government's always gonna need a warrant for all of it. That's a possible reading. And I think the broad picture here, the way I think it's useful to think about it is, what is *Chatrie* really about? It's about not only just devices that we now have, but kind of a new world in which we're constantly, we're kind of living through our phones and records are being created that didn't used to exist. And what do you do with this shift from physical world surveillance where the government could sort of track someone in the physical world but not be able to know wherever anyone is, to a world where actually the government, if they know the person's cell phone number, they can find out all these records about them? The big picture question here is how do we translate Fourth Amendment protections from the physical world, the 18th-century facts of the government breaking into your house and taking away your stuff? How do we translate those principles to the digital world where we've got network communications? Do we say that basically we're gonna have more Fourth Amendment protection to counter the

fact that now there are more records? Are we gonna try to equalize the rules and draw comparisons between the records that exist in the digital world and physical world records, kind of draw analogies between them and say some of those are protected and others are not protected? The Court in *Chatrie* doesn't answer those questions. They don't tell us where we're going. Sort of what's the ultimate big picture here. They give us a hint that it's gonna be broad. The Fourth Amendment is gonna apply broadly, but we just don't know how broadly. And that's something that lower courts now have to figure out.

[00:36:33.5] Julie Silverbrook: At the end of the article, you talk about this idea of *Chatrie* pointing to what you call a world of super privacy in which the Fourth Amendment would restrict the government's access to information more than it would in the physical world. And I do think the language in *Chatrie* is very broad. And casting things in terms of privacy more generally does sort of set us down that path. Explain why you think it's pointing in that direction. Help us understand ways in which I actually think Justice Gorsuch is searching for a way to limit that in his concurring opinion. And of course, Justice Alito just disagrees with that perspective.

[00:37:17.0] Orin Kerr: So the possible reading of *Chatrie* is that the Court is basically looking at the digital world and saying there's just a windfall in how many records exist now, and we need to expand privacy protections to kind of end up in the same place as we used to in the physical world. In effect, more records, but more Fourth Amendment protection over records is maybe the big picture that could be suggested by *Chatrie*. So maybe the answer is in the physical world, yeah, you didn't have Fourth Amendment rights in your numbers dialed, and you didn't have Fourth Amendment rights in what you... Your financial transactions, and you didn't have Fourth Amendment rights in what you told someone. But that's because that was a rudimentary technological world in which mass surveillance was not possible. Now we move into this modern world in which, gosh, there's so many records that could be kept on everyone. Now we're gonna say, yeah, all these records exist, but actually now they're all covered by the Fourth Amendment and the government basically can't do anything without a probable cause warrant. And we don't know if that's where *Chatrie* is going. We don't know, how would that work? Is that actually something that's gonna allow the government to solve criminal cases, or is that something that's gonna so interfere with law enforcement because they usually need some records collection to get to probable cause to allow the warrant? And so basically the technology is shifting and the Fourth Amendment is shifting and we're all kind of watching this to see where does... Do we end up in an equivalent place, or do we end up in a place where there's just more Fourth Amendment protection online than offline and maybe the government has a harder time investigating cases involving online crimes than offline crimes? How does this shake out? That equivalence question, I think, is a really, really important one to keep in mind.

[00:39:20.8] Julie Silverbrook: Let's talk through how would you limit this? Right? So where would you draw the lines in the digital world that would make that landscape feel more analogous to the physical world?

[00:39:34.7] Orin Kerr: Yeah, so in my own scholarly work, I've suggested that we should be thinking of this as an analogy. We should be thinking of the physical world and the digital world and sort of effectively the digital world replacing things that used to happen in the physical world. So in the physical world, I might go to your house and we might have a conversation and the government could see that I went to your house. They couldn't see what our conversation was. And so we should have a Fourth Amendment that kind of in the digital world recreates that, the now, today we might text and the text is protected, but maybe the records that there was a text message sent are not protected. Sort of look at the data and think about data substitutes and try to replace that. That's one possibility. I think it's a possibility that's still open in the *Chatrie* world, mostly through the Court saying, "Okay, maybe, for example, records about communications, the fact that a communication existed, maybe that's not that private."

[00:40:30.3] Orin Kerr: And so it might be that this idea of numbers dialed in the telephone setting could still be applied in the digital world because you'd say, "Well, I sent an email to someone or I texted someone, that's not... The fact of the communication is not that sensitive." And therefore you preserve the telephone old case and you apply it to the new case and you have that equivalence. That's possible. It's not obvious. One answer, this is the real challenge I think of *Chatrie*, is this totally exposed this idea that, okay, if you're gonna start saying what information is private and what's not private, like what's really sensitive and what's not sensitive, you've got to come up with a category of things that are not sensitive. And everything's kind of... There's always the potential of sensitive or non-sensitive information. And so it's really hard to do that, and it might be that they just don't play that at all. They don't do that. They just say, "Listen, all records are sensitive as long as they are digital records held by internet providers, and we're not gonna start looking at which records are sensitive or not." But there are various tools they could look to to kind of figure out what's more or less sensitive if that's something that they want to do.

[00:41:40.0] Julie Silverbrook: What do you think the next big Fourth Amendment case that court watchers and the general public should be keeping an eye out for? Which cases do you think they should be looking for?

[00:41:49.5] Orin Kerr: At the Supreme Court level, there are a couple of circuit splits on how the Fourth Amendment applies to digital evidence collection. A cert petition was just filed a few days ago on the border search exception. Does the government need a warrant to search someone's cell phone as it crosses the border? With physical evidence, the answer would be no warrant is needed. Should that be the rule for cell phones? That's something that lower courts have divided over, and there's a bunch of pending cases on. The big issue, I think, to watch in the lower courts in the short run in terms of what *Chatrie* means is gonna be automated license plate readers. And you've seen a lot of this in the news recently with disputes over Flock camera systems and the like. So how do you tease through the different interpretations of *Chatrie*? Automated license plate readers are one way of thinking through this. Like, what is an automated

license plate reader? Is that a way of determining someone's location that fits that *Chatrie* mold, so it's all a search? And if so, is accessing... Is it the existence of the system that's a search? Is it querying the record that's a search? Is it storing the record that's not queried? Where do you get the search along this, if there is a search, is one way. And then also, what's the limit of that? So if maybe a Flock camera system with a 1000 cameras is a search, is it a search for an officer to just pull out his iPhone and take a picture of a crime scene or take a picture of someone's house? Is that a search? Well, it's the classic law professor question that we love to always ask, where do you draw the line between a massive camera system and just a camera like a cell phone, 'cause that everybody has too? So those are gonna be hard questions to grapple with. But the automated license plate reader cases are pending. There's one in the Fourth Circuit, there's a couple in other places. So that's one to watch in the short run.

[00:43:44.3] Julie Silverbrook: And I think it's going to impact other investigative technologies as well, right? So looking at IP addresses, internet search terms, what other investigative technologies are potentially impacted by *Chatrie*?

[00:43:58.4] Orin Kerr: Oh, I think it's gonna impact a lot. And I think this is something for defense lawyers to raise in lots and lots of technology cases. One of the caveats to that, though, one of the things that makes this kind of a funny mix, is you've got very broad interpretation of the Fourth Amendment at the Supreme Court level, but then there's not much of a remedy in most of these cases for reasons we talked about earlier, this good faith exception to the exclusionary rule. And that means that a lot of defense lawyers are out of practice challenging novel technologies, challenging the government use of these technologies, because this good faith exception is likely to apply at the end anyway. So you have lots of things that could be challenged, lots of things that maybe under *Chatrie* are now unconstitutional, or at least are plausibly unconstitutional. But it's not obvious that you're gonna get a lot of criminal defense lawyers challenging it, because it may be that their clients can't actually benefit from a ruling that it's unconstitutional, and so they're not likely to have the incentive to bring these challenges.

[music]

[00:44:57.6] Julie Silverbrook: Orin, it is always such a pleasure hearing from you about the Fourth Amendment and chatting with you about important cases like *Chatrie*. And thank you for I think revealing the complexities of the case and the possibility that this is really going to fundamentally alter the way in which we apply the Fourth Amendment. So thank you as always for being such a wonderful speaker and educator for our audiences.

[00:45:23.2] Orin Kerr: Julie, thanks so much for having me.

[music]

[00:45:31.4] Julie Silverbrook: This episode was produced and mixed by Bill Pollock with production support from Charles Sahm. Research was provided by Anna Salvatore and Tristan Worsham. This year, there is a question that our team at the National Constitution Center has been asking, as we celebrate America's 250th anniversary. And we look to the Constitution's 250th anniversary in 2037 and the Bill of Rights 250th in 2041, the question we keep returning to is, what will future generations say that we chose to build during this decade of milestone anniversaries? I'm excited to share with you that we've launched a new Substack which will explore this question. It's called *The Civic Decade*. This is a moment to not simply celebrate our constitutional inheritance, but to strengthen the institutions, civic habits, and constitutional culture that will determine whether it flourishes for another 250 years. Join us on Substack, civicdecade.org. Please recommend We The People to friends, colleagues, and anyone anywhere who's eager for a weekly dose of constitutional education and debate. And as always, remember the National Constitution Center is a private, nonpartisan nonprofit, and we rely on your generosity, passion, and engagement for all of our programming, including this podcast. Please consider donating today at constitutioncenter.org/donate. On behalf of the National Constitution Center, I'm Julie Silverbrook.