What Trump Can Teach Us About Con Law
The Capitol Mob and their Cell Phones

Roman Mars [00:00:00] Okay, so it is March 2021. What are we talking about this time?

Elizabeth Joh [00:00:04] The violent attack on the Capitol happened more than two months ago. And if you remember, Trump's followers took their “Stop the Steal” advice literally, and hundreds of people violently breached the barricades of the Capitol. They fought with the police, and the mob stopped the counting of the Electoral College ballots for several hours because members of the House and Senate had to evacuate their chambers. Five people died, and more than 100 people were injured. And that includes an officer who lost an eye, concussions, and cracked ribs. And so, it's really hard to understate how incredibly violent things became. Now we know something like 800 people were part of that January 6th attack on the United States Capitol. But fewer than 40 people were arrested on that day, though. So, in other words, nearly everyone who stormed the Capitol was allowed to leave. And we know that dozens of people tried to hide their participation in the riot later, either by deleting their social media accounts or trying to smash or, in one case, even microwave their cell phones. And so far, more than 300 people have been charged in federal court for crimes related to the Capitol riot. Now, there are some people who've been charged with some very, very serious acts, like assaulting police officers. But if you look through the dozens of criminal complaints that have been made public, many of those who have participated in the Capitol riot had lesser roles. Don't get me wrong, everyone there wanted to stop a constitutionally mandated process. What I mean is that many, many of these defendants have been charged with less serious offenses, like entering a restricted building or disorderly conduct in a restricted building. They're all federal crimes, but they're less serious offenses. And federal prosecutors have made it clear that they're not finished. And so, for example, in a filing from March 12th, federal prosecutors said the investigation and prosecution of the Capitol attack will likely be one of the largest in American history, both in terms of the number of defendants prosecuted and the nature and volume of the evidence. So, they said that they expect something like 100 more people to be charged eventually. But remember, most people weren't arrested on January 6th. So how exactly did the FBI find these people and link them to the attack? Well, some of them in the mob that day were pretty easy to spot because many of those people, it turned out later, had posted selfies or live streamed themselves on social media.

Roman Mars [00:02:46] That's right.

Elizabeth Joh [00:02:47] Or in other cases, people were identified by friends or neighbors, college classmates, family members, from pictures on social media or from the photos and videos that the FBI has posted on its own website. In some cases, we've seen these voluntary internet sleuths identify people. There was an Olympic swimmer who was identified by his Olympic jacket that he wore that day. Leo Brent Bozell IV is the son of a prominent conservative activist. He's also the grandson of one of the most important figures in the conservative movement of the 1950s. He was identified by a sweatshirt he wore, which had a Hershey Christian Academy logo. But it's not enough for the government to show that a person was just identified on social media in order to build its case. Instead, you'd want evidence about what the person did on January 6th and further proof that they were there at the Capitol. And from what we can tell from the publicly released documents, the FBI is relying on techniques that pick up on the digital trails of suspects in ways that they probably didn't realize were possible. How? By tapping into the vast amount of digital information we're all leaving behind everywhere we go and relying

on tactics that the courts are struggling to define and limit when it comes to the Constitution.

Roman Mars [00:04:18] Cool. So, you're going to make me uncomfortable about prosecuting people I hate?

Elizabeth Joh [00:04:26] Not necessarily. I'm going to make you question, you know, government power. Let's put it that way.

Roman Mars [00:04:31] Sounds good.

Elizabeth Joh [00:04:32] Okay.

Roman Mars [00:04:52] This is What Trump Can Teach Us About Con Law, an ongoing series where we take the current events surrounding the former president and use them to examine our Constitution like we never had before. Our music is from Doomtree Records. Our professor and neighbor is Elizabeth Joh. And I'm your fellow remote learning student and host, Roman Mars.

Elizabeth Joh [00:05:23] Let's start with the Constitution's Fourth Amendment, which regulates how the government conducts searches and seizures. Not everything we say, do, or possess is protected by the Fourth Amendment. The Supreme Court has said that the Fourth Amendment protects our reasonable expectation of privacy. But if the government interferes with what the Supreme Court has decided is a reasonable expectation of privacy, then it has to follow the other rules of the Fourth Amendment. Now, in the usual way of doing things, we assume that the police have to get a warrant--think of that as judicial authorization--based upon probable cause to conduct a search. Probable cause is the level of suspicion the government has to establish in order to perform a search or seizure; it comes right from the language of the Fourth Amendment itself. So, for instance, here's an easy example. The government usually needs a warrant based upon probable cause to enter your home to search it, or a warrant based on probable cause to search your laptop. But sometimes the government doesn't want to enter your home. They want to know where you've been so they can tie you to a place where a crime occurred. What's an easy way to find out? Your cell phone. But if you have a cell phone, that cell phone is also continuously scanning for the nearest cell phone tower to find a signal. We all want good cell phone service, right? Well, that means that these cell phone towers--they're sometimes called cell sites--and your phone are communicating with each other several times every minute, even if you don't use your phone. Now, each ping from your cell phone to a cell site means a timestamped location specific record. That's called "cell site location information." So, if the government collects all the cell site location information for your phone, that means the government has a pretty good map of where you've been. So, in the 2000s, the police began to collect this information in criminal investigations. They'd asked cell phone service providers for days, weeks, sometimes months of cell site location information to identify the whereabouts of a person they thought was connected to a crime. But they wouldn't get a warrant for that information. So, Roman, what could I learn about you if I followed your cell phone data?

Roman Mars [00:07:50] Oh, Lord. Well, you would mostly learn that I spent a great deal of time inside my own home. But you would learn, like, my favorite place to run on the afternoon, which is across the bay. You know, like, you would find... mostly those two things.

Elizabeth Joh [00:08:13] Good. I mean, we learn a lot, right? We learn a lot about your habits. So, if the government can find out every single place you've been to, they're not just learning about particular places. We can make inferences about lots of things: who your friends are, where you like to hang out, maybe your religious beliefs, whether you're doing things that aren't necessarily illegal but you don't really want the government to know about. So, this is the constitutional problem with cell site information. Even though it became used more heavily by the police in the 2000s, it didn't easily fit into the categories of things that the Fourth Amendment usually protects by requiring a warrant. So, here's what I mean. First, all that pinging between your cell phone and the closest cell tower--most of that happens in public spaces. And the Supreme Court has long said that your movements in public aren't protected by the Fourth Amendment. Anyone can follow you. There's a second problem. The Supreme Court has also said that the Fourth Amendment doesn't protect records you hand over to a third party--a third party like your cell phone service provider. You choose to do that--that's the rationale--so you're also giving up your constitutional protections. Now, if that location information from your cell phone falls into either one of these two categories, that means you don't have any constitutional argument against the government collecting it as much as it wants to. And the Supreme Court finally decided to weigh in. Now, in 2011, the police arrested four men who they suspected of being involved in the robbery of cell phone stores in Michigan and Ohio. Now, one of them confesses--says he's part of a big group of people who've been involved in these robberies. And he gives the police some of the group's cell phone numbers. So, prosecutors were then able to get the cell site location information for several of these robbery suspects, including for a guy named Timothy Carpenter. Prosecutors asked for more than 150 days' worth of Carpenter's records--where he'd been all those times. Now, those records, it turns out, places Carpenter near the robberies when the robberies occurred. Carpenter's argument was that, you know, the government can't use these records in his prosecution because the government never got a warrant to obtain those records. So, in 2018, the Supreme Court decided that even though these cell phone records traced Carpenter's movements in public, and even though the records were not in Carpenter's own hands, the government would still need a warrant before it could have those records turned over. Now, Chief Justice Roberts, who writes the opinion in this case, tells us that there have been what he calls "seismic shifts" in digital technology. And those shifts made it possible for what he called "the tracking" of not only Carpenter's location, but also everyone else's, not for a short period, but for years and years. So, he's basically making this point that cell phone records of a kind that they got in Carpenter's case--they're nothing like actual human police officers following Carpenter around because let's face it, there's no police department that can just have someone tracked 24 hours a day for, you know, days or weeks at a time. And what do you do when you get the cell phone location information? Roberts says that the government--when it has this capability--they are able to conduct what he calls "near perfect surveillance as if it had attached an ankle monitor to the phone's user." The problem is, at least from the Supreme Court's point of view in this case, that if any of us want to live in the world today, we're forced to accept creating a trail of digital breadcrumbs. And the Supreme Court in the Carpenter case says, "Only the few without cell phones could escape this tireless and absolute surveillance." That pretty much means no one can escape. So, Carpenter versus the United States was a huge decision because the Supreme Court was weighing in on the government's reliance on this new technique that was made possible by the digital world. Now, no one really thinks about how their need for a reliable, you know, easy-to-get cell phone service can also mean that their movements are tracked and analyzed by the government. But in Carpenter, the Supreme Court tells the government, "You're going to need a warrant for that."

Roman Mars [00:12:48] If getting a warrant is the bar that we're talking about, getting a warrant doesn't seem all that difficult for most law enforcement.

Elizabeth Joh [00:12:55] Yeah. So certainly, the warrant requirement--it's not as if that's impossible to do--but it's really a comparative thing. You know, when you have a warrant requirement, the government, at a minimum, has to come up with some set of facts--"This is why we want to focus on this person"--as opposed to needing no justification at all. Like, "Why not you as opposed to anybody else?" It's just another kind of limit on government action.

Roman Mars [00:13:17] It just seems like a limit that so far, we have not found was extremely limiting when it came to, you know, the enforcement of law.

Elizabeth Joh [00:13:28] That's right. But trust me, if there were a choice between "Do I want a warrant requirement in a case against me or none?" you'd want that warrant requirement.

Roman Mars [00:13:35] Of course. Oh, absolutely--I mean, from our point of view of a person. But from the point of view of law enforcement, it doesn't seem like this is a gigantic hurdle, even though it was one they don't want to have to jump over. But it doesn't seem like a big one. Am I getting this wrong?

Elizabeth Joh [00:13:51] No, I mean, it's not that it's impossible or it's really, really difficult, but it does then cut out the people for whom the government only has, like, a weak case or a minimal case. You know, a judge just isn't going to accept that.

Roman Mars [00:14:03] Right. Okay. So how does the size of the mob at January 6th... I mean, they all did have cell phones on them. I saw a lot of the streams and various things and the pictures. How does this tie to all that?

Elizabeth Joh [00:14:15] Well, it does in an indirect way. In the Carpenter decision, the Supreme Court was looking at Carpenter's case, where the government was looking very specifically at Timothy Carpenter's records. And then in doing so, they said, "You know, this is a very narrow decision we're making. We're making a decision about long term cell phone location information collection by the government." But in Carpenter, the Supreme Court also specifically says, "There's also other stuff that the government is doing that we're not going to be deciding today, including cell tower dumps." You ask, "What is that?"

Roman Mars [00:14:47] Yeah. Well, okay.

Elizabeth Joh [00:14:48] A cell tower dump happens when the government says to a cell phone service provider, "Tell us every device that tried to ping this particular cell tower at this time."

Roman Mars [00:15:00] Hmm.

Elizabeth Joh [00:15:01] So if you look at some of the court filings in the January 6th cases, it kind of looks like that's what the government did. So, in other words, it looks like they told some of the cell phone service providers, "Get the numbers of everybody who pinged the cell tower that includes only the Capitol building. Then you use that to identify people and to build a case." So, the language you see in some of the cases is that the government "lawfully obtained cell site records." Now, it looks like in the January 6th case,

the government is using warrants. But the point that I'm trying to make here is that in Carpenter, the Supreme Court said, "We don't have anything to say about that particular technique--cell phone tower dumps. We're going to wait for another time to do this." And in fact, there's some disagreement in the courts below the Supreme Court as to whether or not the government really needs a warrant or not. Now, this also leads to another kind of information that the government has collected in some of the Capitol riot cases that we should also talk about. So, Roman, do you use Google?

Roman Mars [00:16:07] Oh, yes, I would say that I use Google quite a bit.

Elizabeth Joh [00:16:09] Yeah. Well, chances are that you are creating a long, detailed record of your location for Google. So, Google has a feature called Location History. If you've turned it on--and you probably do if you use things like traffic alerts or location tags for your pictures--then Google collects your location history as long as you're signed into your Google account. Google can collect this even when you're not using your Google apps. Now, how can they tie this to location? Because Google can calculate the latitude and longitude of your cell phone by using information from nearby cell towers, GPS signals, Wi-Fi networks, Bluetooth devices. Now, Google records the margin of error for how close you are for that calculation as the map's display radius. So, you're also giving Google location data lots of times when you conduct Google searches or use Google Apps that have location enabled. So, remember, if you're a Google user, Google has everything associated with your account. That's your name, your address, your telephone number, everything. So, all that convenience--like you want to figure out, like, what's a restaurant near me where I can order dinner tonight--that also means that you're telling Google exactly where you are all the time.

Roman Mars [00:17:25] I mean, other than providing me these great conveniences that you've mentioned, why does Google say they need this information?

Elizabeth Joh [00:17:32] Well, Google claims that it wants this information for targeting ads, right? To see how well those targeted ads work. So, if Google serves you, Roman Mars, an ad for a particular thing for a store and then it sees that you walk into that store--hey--that's a successful ad, right? But it turns out that it's also really useful for the police to have access to all this location data.

Roman Mars [00:17:55] Sure.

Elizabeth Joh [00:17:56] So this is a more controversial use of information than what we have seen in Carpenter largely because we don't really have a definitive answer about this in terms of constitutional law. So, remember that easy example of the warrant I gave you, right? The police usually need a warrant to search your home, presumably to look for evidence of a crime to which you might be associated. But what if the police apply for a warrant to see which people have been at a certain place and time without having any particular person in mind? Now, that's called a "geofence" or a "reverse location warrant," and they're pretty new. So, in these cases, the government might ask a judge to authorize a warrant to get data from Google to see who was in an area where a crime took place. They don't know who they're looking for. Why Google? Because Google is Google. Google has all of this location information from millions and millions of people. Now, here's what appears to happen with these reverse location warrants... Google responds to the warrant by providing information about every single device that was at the time and place specified by the government with anonymous identification numbers. Then what next seems to be happening is that the government then looks through all that information to see if they see

some kind of pattern or any way to narrow down all of the devices that have been identified. And then they say, "Okay, here's a smaller list, Google." And then presumably Google will then reveal the identities of the users that the government wants to look for.

Roman Mars [00:19:34] So is this what they did in January 6th?

Elizabeth Joh [00:19:37] Well, the government hasn't said, "We used a Google reverse location warrant." But if you look at some of the Court filings, you see a lot of clues that the government probably used this technique. And here's what I mean. So, in one case, the government says they identified a particular defendant as being inside the Capitol during the riot by what they called "records obtained through a search warrant served on Google." So, in that case, the government says that the defendant's Gmail account was present at the Capitol during the riot. So, what if the public filing says, "Google location data shows that a device associated with"--and they name the defendant's Gmail account--"within the U.S. Capitol at coordinates associated with the center of the Capitol building, at 2:56 p.m. In another case, the government even provided a map of data points where that Gmail account was moving around inside of the Capitol building.

Roman Mars [00:20:35] Wow. Wow.

Elizabeth Joh [00:20:36] Now, when they describe what they're doing, the government also says that the Google records show the maps display a radius of 34 meters. That's the margin of error about longitude and latitude that I just talked to you about before. So, the government also says in these documents that the defendant's Google account is not among those they have listed as devices associated with people authorized to be inside the Capitol. So, all of this sounds very much like the government did, in fact, rely on a geofence or what's called a "reverse location warrant." So basically, they asked Google to identify everybody who was a Google user within the Capitol on the day of the attack. Then they have another list of people who are allowed to be there--Congress, their staff, law enforcement. And the ones that remained are very likely to be people involved in the riot.

Roman Mars [00:21:28] That's interesting. Why is it fundamentally different than, like, getting the surveillance tapes of the Capitol and combing through those to see who's there?

Elizabeth Joh [00:21:38] That's a good question because in pictures of people's faces--presumably the way we thought about that in the past is you are kind of exposing your public face in a public place for which you have no protection. Although I should say even that is becoming increasingly a contested argument because of facial recognition technology that's really easily available and there are lots of privacy and civil liberties folks who say that's not obvious either--that that should go without protection. Here, I'd say the problems go one step further because this is a search warrant based on probable cause. But the Supreme Court hasn't yet decided a case like this. And it brings up questions about the way we think warrants usually work because in a reverse location warrant, the government's saying, "Look, we have probable cause because a crime happened in this place and at this time. We don't know who we're looking for. But Google will have user information that will point to somebody that we don't know yet who might be involved in the crime." So, a lot of people are saying it's not clear that this is constitutional because it doesn't look like a normal warrant as required under the Fourth Amendment because what happens is Google responds by scooping up the information of everybody. It becomes a kind of all persons search warrant. We want to find everybody. So that means that your

location data gets collected because you happen to be in a particular place at a particular time. Now, the January 6th defendants aren't particularly sympathetic--number one, because they were part of a mob and they tried to stop a constitutional process. And number two, if you think about the Capitol on that day, there were only certain people allowed within the building on that day. It wasn't a truly public space. So, if we can identify the people who weren't authorized to be there, everybody else was pretty much trespassing; they were committing a crime. But the Google reverse location warrant--when it's used elsewhere, like, let's say, for example, the police want a list of every Google user within a 12-block radius of downtown Oakland because they're looking for a robbery suspect... That's going to scoop up lots and lots of information on totally innocent people, who had nothing to do with it, which can lead to wrongful arrests. And we do know of some wrongful arrests that have been the result of these reverse location warrants. It can just lead to the fact that the police might use this kind of technique to find information on people for maybe the wrong reasons. They might have a reverse location search warrant for protests. And, you know, that might scoop up information of people who don't want to be targeted by the police simply because they've been involved in a protest. So, the January 6th use of this might not be so worrisome for some people. But the larger technique I think is certainly raising all kinds of questions.

Roman Mars [00:24:48] Yeah. I mean, it seems like one of those things where the scale and scope of the dragnet really matters.

Elizabeth Joh [00:24:53] Well, that's absolutely right. I mean, I think one of the biggest things that, you know, these kinds of techniques are telling us is that, you know, just how much personal information about our habits, our friends and associates, what you do and when you do it, is just being constantly collected all the time and then being used for reasons that most people would never, ever have expected. And again, they probably don't even realize now the extent of information they're able to turn over. So, if you think about this, you might say, "Well, what's the big deal about it?" It's a little bit different if you think, for example, you know, what if there's been Black Lives Matter protests? We know that journalists reported that the police in Minneapolis used a reverse location warrant during the protests, after the killing of George Floyd last year, they said, "Oh, we need to identify people who were involved in vandalism." That seems reasonable. But if you have a reverse location warrant, then you're scooping up the information of everybody who is there. And it is, as you say, a huge dragnet that potentially exists. Should we be happy that the government has been able to identify so many of the people who took part in an attack on the nation's capital? Yes. Should we also worry that the government has easy access to all of these digital trails? Does this raise questions about what our digital privacy looks like in all of these kinds of criminal investigations? Also emphatically, yes.

Roman Mars [00:26:19] Yeah. Yeah, it's always that way. This show is produced by Elizabeth Joh, Chris Berube, and me, Roman Mars. You can find us online at trumpconlaw.com. All the music in Trump Con Law is provided by Doomtree Records, the Midwest Hip hop Collective. You can find out more about Doomtree Records, get merch, and learn about their monthly membership exclusives at doomtree.net. We are a proud member of Radiotopia from PRX, supported by listeners just like you.