BROKEN LAW - Episode 54
"Preparing for Abortion Surveillance in a Post-Roe World"
Released on June 14, 2022

TRANSCRIPT OF EPISODE

JEANNE HRUSKA: Welcome to Broken Law. The podcast about the law, whose interests it serves and whose it does not, brought to you by the American Constitution Society, a 501(c)3 non-partisan, non-profit organization. I'm Jeanne Hruska, senior advisor for communications and strategy at ACS.

As we record this, we are awaiting the Supreme Court's final decision in *Dobbs V. Jackson Women's Health*. And if Justice Alito's leaked draft opinion is any indication, the final decision in that case is likely to overturn *Roe v. Wade*, resulting in the banning of abortion in more than two dozen states.

In anticipation of this post-Roe world, there's growing conversation about how states with abortion bans can go about investigating whether someone has had an abortion. This has given rise to the notion of abortion surveillance, a harrowing concept and yet something that could soon be all too real for those of us with uteruses.

To discuss how abortion surveillance could work and what is being proposed to counter it, I'm joined today by one of my favorite privacy gurus, Chad Marlowe, Senior Policy Counsel at the ACLU where he principally focuses on privacy, surveillance and technology issues.

I do have to note my only concern going into this recording is that I almost always come away from conversations with Chad even more paranoid than I already am about mass surveillance. But, these are the times in which we live. Chad, welcome to Broken Law.

CHAD MARLOW: Thank you. It's good to be with you.

HRUSKA: How are you doing?

MARLOW: I'm good. I'm doing okay. But, as you say, we unfortunately we live in a world where you know, whenever we get kind of in a moment where we go, "Well, I

guess this is about as bad as it can get," the world kind of doubles down and certainly the Supreme Court's potential overturning of *Roe v. Wade* would be such a dramatic and almost inconceivable moment for our country.

HRUSKA: So before we talk about abortion surveillance specifically, I want to just talk digital surveillance more broadly, because it's something that I think we're familiar with but we may not understand the nuts and bolts of it. The technology that enables abortion surveillance is not unique to abortion, and it is ubiquitous in our everyday lives. So, talk to me about this when we say digital surveillance? What are we talking about?

MARLOW: I would put abortion surveillance into two categories. The first is the technological surveillance of your data. And the second is the technological surveillance of you.

So, when we're talking about the technological surveillance of your data, you can think about anything that you put into electronic form kind of creates a print, where you know, outsiders, those who are authorized and those who are not authorized to get access to your information. And that really happens almost constantly in your daily life in the 21st century.

So you wake up in the morning, and you watch a TV show on your television on Hulu, and what show you watch is tracked by both the person who provides access to your internet and by Hulu or whoever the provider is who provides access to the show you're watching. Then you decide to go on the internet and read a newspaper and your internet service provider in that newspaper are going to know that you went to that newspaper, they're going to know what article you read. Certain trackers can even find out which particular paragraphs you hovered over for longer to know what you're thinking. The day goes by, you do your work, you shoot some emails to people well, if you're not using a secure email server, your emails can be tracked, both the fact that you're writing and sending them to someone, and in certain contexts, the actual contents. You then go online and order lunch. Well, now we have access to what lunch you ordered, which may not be that private, but now we know where you live because that's where the driver is being sent to. God forbid you take a break from work in the afternoon to go to a doctor's appointment. Well, if you get a ride share like a Lyft or an Uber, well now, we can use the data sharing that that company uses to track where

you're going to know that you left your house at a certain time. You were at your doctor at a certain time. And if you happen to use a car coming back, we can estimate exactly how long you were at your doctor's office. You're then on the way home, you go on your phone, you send a text or you send an email, you do a little searching of Facebook and Twitter and Instagram. All of those things are captured online. It's almost impossible to share data from one person to another without it going through intermediaries. Again, be it your phone provider, the people who provide your internet access, your search engines, your actual web browsers, they all have the ability to track you.

The physical side of the tracking is with tracking devices or surveillance devices that are out in public. So, for example, your kind of standard surveillance cameras that are out there and watch where you go. If they have facial recognition attached to them, not only can they watch where you go, but they can identify you and who you're with.

HRUSKA: You mentioned standard surveillance cameras. We're used to thinking of surveillance cameras in association with specific parts of the world, for instance, in London or in parts of China. You literally can't take a step in London without being caught on camera. We don't think of surveillance cameras as ubiquitous here in the United States. So, talk to me about the breadth of camera coverage here. Increasingly I think of the Rings that people have, the doorbell Rings with cameras that people are putting on their front porches. Are those included when you're talking about surveillance cameras?

MARLOW: Yes, they can be. You could lump surveillance cameras into three categories, right? You have government surveillance cameras, which are ones that are actually operated by and watched by the government. For example, your local police department has cameras up around your city and your local Department of Transportation has red light cameras. Those are your government cameras. All the information captured by those cameras goes directly to the government.

The other two types include business cameras, where you have like a bank or a bodega, with security cameras.

HRUSKA: Private security cameras?

MARLOW: Right. In most instances, the government doesn't have direct access to those, but they can go to a business owner and ask for it or they can get a warrant and get access to it. I'm going to put a little pin in that for a moment and return to that.

The third kind are your private, individual. or home surveillance cameras like ring. Again, those do not go directly to the government. They go to the homeowner, but the government can come and ask for the footage that you're filming. Now the reason why I say you put an asterix by the last two categories is there have been recent efforts by governments to incentivize people to give them direct access to your cameras.

One of the worst programs I'm aware of in the country is in Detroit, Michigan, where they have a program called Project Greenlight. And it's named for that because whoever enrolls in this program actually puts up a green light above their surveillance camera, but what they say to these business owners, which is so odd to me, is they say, "if you give us direct, automatic and even live access to your cameras, we are going to give you priority 911 service." I thought all 911 service was priority 911 service, but here, police will patrol your business area more often, you will be able to talk directly to the police on a regular basis to talk about your concerns. So basically, what they're doing is, they're pulling back services that they used to give to everyone and now just doling it out to those who will cooperate by turning their private cameras into government surveillance.

HRUSKA: You're paying for government response with your privacy. If you're willing to forsake your privacy rights, then we'll give you priority response to 911 calls.

MARLOW: More realistically, you're actually treating the privacy of others, customers of for instance, who are not getting a benefit by the way. So yeah, so there is an increasing effort by government. They also do this with Ring by the way, where Ring will make a deal with police departments. If police go out and try to promote the product, Ring will then share with them information on who buys the product. So it's easier to contact them when you're looking for information. So there's constant efforts to kind of break that line between government cameras and private campus.

HRUSKA: All right, two questions based off of everything you just said. The first one is: part of the concern here is how much data is captured without us thinking about it and without some folks even realizing it. Right? Every time you open an app on your

phone, there is a record of that but I don't think most people open an app on their phone and think "what I'm doing right now is being tracked." If I have a private photograph in my house, I'm aware that I have it and when somebody walks into my house and looks at that photo, I'm aware that they're looking at the photo. With digital data, you do not know who all is looking at your data, because it's not in your physical possession. Is this making any sense?

MARLOW: Perfect. So I want to answer your questions. I want to start by explaining why I hesitate to answer this question. Surveillance is oppressive. When you feel you are being surveilled, it really inhibits your freedoms and your human rights as a human being. If you don't believe me, talk to people who lived in East Germany in the Cold War under the Stasi, talk to Muslims who live in western China nowadays, talk to Black Lives Matter leaders in the United States. So, this is going to hurt a little bit when I say this. But the fact of the matter is, you're being surveilled all the time. And you not thinking about it is the ideal situation for the people who are surveilling you, be it the government, be it companies who want to collect your data in order to sell you more things.

HRUSKA: They want you to be ignorant of what they're doing. They want you to not know about it.

MARLOW: Unfortunately, you know, into the category of people who now have to be scared is anyone seeking reproductive rights services in this country if *Roe v. Wade* goes away. Unfortunately, it's a little bit like, not to mix my metaphors, but it's a little bit like the Matrix when Neo takes, I have to get the right pill here because I'll offend people, when he takes the blue pill and then he sees everything, right? Unfortunately, people who are going to be in need of reproductive care need to swallow the blue pill, and we need to show them what the matrix really looks like, so they can protect themselves.

People need to understand what this surveillance looks like post-Roe. People need to hear the words to know how scary this is because if you get an abortion, you are going to be charged with murder.

HRUSKA: In some states.

MARLOW: Right, if you drive someone to a Greyhound bus station so they can travel to another state to get the abortion care they need, you can be charged as an accessory to murder. I mean, these are not a slap-on-the-wrist charges. These are life and family destroying charges. And so, people unfortunately, in the world we're moving into, are going to have to learn to reflexively protect themselves. Because one mistake could be the difference between you know, your liberty and being in prison.

HRUSKA: One more question about everything that you talked about in the beginning and that is the motives of the people collecting the data. You started off by talking about Hulu. And when I think of Hulu, I don't think of a malicious company. I don't think necessarily of a progressive nonprofit, but it's not the same to me as Facebook or some companies where I'm cringing at the amount of data that company may have on us. So I want to make this distinction. Some think, "Yeah, someone knows what I watch, not a big deal. Who cares?" Why is that the wrong mindset? If you know, Amazon knows this about me and my weather app knows that, who could be accessing all of that information other than the company in question.

MARLOW: So first of all, just to be fair, I'm not picking on Hulu, I'm just a customer.

HRUSKA: Right. I say Hulu only because you brought it up earlier. The same could be said for Sling, for your internet service provider.

MARLOW: Right, any one of those companies. There's many reasons we should be concerned about who has our data. One of which could just be, you know, embarrassment about wrong assumptions, right? Like, I decided to binge watch Sex in the City, and suddenly I get advertisements for sexual enhancement devices and bars, right. They can over assume things.

But more troubling is that it does not take a lot of data points to be able to predict the thinking and behavior of a human being. Now that sounds odd, right? But understanding 25 key facts about Chad Marlow is going to enable these companies to predict with really almost stunning accuracy, my interests, behaviors, and choices in life. Knowing what shows I like to watch on TV, knowing what advertisements I fast forwarded through, versus I actually watched. Knowing what time I watch TV says what time I'm home, what time I leave the home. There's a lot of information that can be gathered from that and so each individual data point seems very harmless, but the more

of them that you collect, the more it gives this incredibly intimate, personal and shockingly accurate portrait of who you are at your essence as a human being.

HRUSKA: And I think this gets to one of the other, really malicious factors with digital surveillance, which is the sharing of your data. Again, my birth certificate is here in my condo, I have one copy of it. If I were to hand it to somebody- Yes, I could make photocopies of it, I could scan it, but in its physical form, I have only one copy of it. I can generally control whether it's going to get duplicated and shared or whatnot. Hulu? I have no idea what it is doing with all the information it knows about me. Again, we're not picking on Hulu for other any other reason than Chad mentioned it. You could use any digital company. They possess a copy of my data, and they have no obligation to inform me of what they are doing with my information, which means they could be selling it, they could be sharing it with the government, and I would have no idea.

MARLOW: If you think about what Hulu does, right? Hulu is not in the business of providing me with television services. It's in the business of making money. Television services are the way it makes money. Well, you know what is worth even more than the television.

HRUSKA: My data!

MARLOW: That's right. If I decide I want to watch *Laverne & Shirley*, perfectly good program, Hulu will make money off of my subscription and off of the advertisements they show me, but they get that money for that month, they get it one time. But the data they collect, they can sell that over and over and over again to people. They can also use it to tell their advertisers, "Hey, you know what, if you're looking for a 50-year-old man who lives in New York City? Boy, have we got someone for you."

HRUSKA: I think Facebook is an even better example of this because you can target ads on Facebook, and you can target who sees an ad based on almost every category you can imagine: age, gender, location, occupation, all of that. And so, the more Facebook knows about you, the more valuable you are because it allows people paying Facebook to target you with advertising.

MARLOW: That's painful to say because some of that advertising targeting is done in very inappropriate ways. So for example, if I'm selling homes in a white neighborhood,

well, I'm not advertising to non-whites. If I'm offering variable rate, high-interest mortgages that I think will only be appealing to people with bad credit, right? I target people with low income, right? I use stereotypes, right? And I say, "Well, heck, let's target Black and Brown communities as well." And so, yeah, there's many many layers of problems with collecting your data, and then, you know, using it to target you. And by the way, it's very important to know all of this is done without asking your permission. And the reason they don't ask your permission is they don't want you to say, "No." So they don't ask and they fight efforts tooth and nail that would require them to ask your permission, which is kind of odd, because it seems like, at a minimum, a basic courtesy but I guess, you know, looking for basic courtesies in 2020 is like looking for a four leaf clover. Good luck.

HRUSKA: I want to address one last question. Before we get into the specific topic of abortion. And that is to address what you and I have heard so often when we talk to people about privacy, which is this notion of "I have nothing to hide." "Why do I care who sees my data?" I hear this all the time, and it makes me cringe. Address that issue, why should people care even if they "have nothing to hide."

MARLOW: So privacy is not about having something to hide. It's not about doing something bad and not wanting to get caught. Although we will be soon shifting to abortion where unfortunately, that is going to be considered something that's bad and illegal, but let's stand back from that and look at different things.

There's two kinds of ways I break up this discussion that resonates with people. You can have someone who is extremely private, who just simply doesn't like sharing information about themselves, and they are going to have a certain standard of privacy, and they, if empowered to do so, will take privacy as far as they can. Let's look at other extreme, Kim Kardashian. People think Kim Kardashian has no interest in her own privacy whatsoever. She puts her entire life online, right? That's not true. Many years ago, Kim Kardashian was at a hospital, I believe in Los Angeles, and someone who worked at the hospital took a picture of her medical chart and posted it online. She flipped out, rightly so. Now you're thinking, Kim Kardashian flipping out about her privacy? Yes, it's just her line is at a different place than yours might be. There's nothing illegal about going to a hospital when you're sick. And it's not that she's actively thinking, "I need to hide my medical records," but she doesn't want them published online. And so, we need to understand that people need to be empowered to decide for

themselves. You know, it's not a question of where that line falls on doing things that are bad or having something to hide, but just people's own sense of self and where they are comfortable sharing and not sharing information.

More specifically, two examples come to mind. You have a bunch of kids in high school who have a day off, they decide to all go to the beach together. They're in their bathing suits. They're having fun. They want to post those pictures on social media, but to their private accounts. They may not have a problem with their friends seing those pictures, but maybe they don't feel comfortable with their teacher seeing them in a bathing suit. Being in a bathing suit on the beach is probably the polar opposite of doing something wrong. Right? If you're in a ballgown at the beach, that's a little odd, but there's nothing wrong with wearing a bathing suit. But they still may not want their teacher or and school administrators to see those photos.

Similarly, you could, after a long week of work, you could go out with your work colleagues, and you could decide to go to a bar and drink alcohol or if you're in one of the 19 states where it's legal, you could use cannabis products. Someone grabs their phone and films it, and you're a little bit stoned or drunk or not at your best. There's nothing wrong with doing that. We're talking about legal activities, but you may not want your employer seeing videos of you in that condition. Again, it's not that you had something to hide per se, it's just that there's a group of people you're okay with seeing that and a group you're not, and you should be able to draw the line.

So that's what privacy is really about. It's about being able to draw that line where stuff is either totally private, semi-private in what you share with a small group, or public where you really don't care who else sees it. And it's those gradations of opinion and the ability to effectuate them, where the privacy discussion really is most centered.

HRUSKA: That's a really good pivot point to talk about abortion surveillance specifically, because this notion of "I've done nothing wrong, I have nothing to hide," also presumes that the law is going to stay the same. On Tuesday, I've done nothing wrong. If on Wednesday, *Roe* is overturned and suddenly abortion is banned in your state, what is deemed right and wrong has suddenly changed. And what you may think of as private may suddenly change. Your visit to Planned Parenthood was absolutely fine yesterday. Suddenly it's going to be suspicious activity in states with abortion bans. And this is part of the reason I grimace when people say, "I have nothing to hide." You

don't know what's going to happen tomorrow. And the information that you are volunteering today may be relevant tomorrow.

MARLOW: Yeah, it's a fact of life that everything that is illegal, is not wrong. And everything that is legal, is not right. And I can tell you, it is absolutely my personal view, and it is absolutely the ACLU's personal view that no matter what the Supreme Court says about *Roe v. Wade,* no matter what laws states may pass, getting reproductive care is not wrong under any circumstances. And it is going to happen regardless of the laws, although it's going to entail a lot more risks and so you know, even your own standards of decency and morality may not line up with what the law tells you it is. And, I'm not advocating for people going out and breaking laws willy nilly without considering them, but there are certain laws that are going to be immoral, and I think that the idea of turning women and other people who seek abortion care from human beings into incubators is sick. There's no other word for it. It's sick. And you know, if I was more eloquent, I would certainly call it antiquated.

HRUSKA: I think sick is the appropriate terminology. It's grotesque. It is inhumane. It is so, so wrong, which is why I think it's so important to talk about this concept of abortion surveillance because this is the world that we may soon live in. So we've just talked at length about digital surveillance, talk to me now about how that is used for abortion surveillance.

MARLOW: So, the challenge with abortion surveillance is- The way that I think about it is that there's two tiers of abortion surveillance. The first one is the surveillance that enables law enforcement to identify you as someone who either got an abortion or assisted someone getting an abortion. They don't need to prove anything, they just need to get enough to establish probable cause that you engaged in the activity. Now, the reason that is important is once you establish probable cause that a person has broken a law, privacy gives way to a judicial warrant process in which they can completely invade your life to look for evidence that you've committed a crime. So where abortion surveillance in the first instance is so troublesome is in the establishment of probable cause.

I'm going to give you two examples where abortion surveillance could be used to find probable cause. The first is period tracking apps on your phone. If you are using a period tracking app, and you are diligently putting in when your period starts every

month and then it stops for two months, and then restarts, is that standard enough to establish probable cause that you got an abortion? I don't honestly know, but three months, four months? Yeah, maybe now it is. And the information you are entering into your app on your phone means that the government could go to that company and say, "Can I take a look at that?" Or if that information is sold to third party data brokers, the government can go and buy it, or they could buy it directly from the app. If the app doesn't promise you to keep your information secret as a condition of using the app then they haven't promised to privacy. And they can go ahead and sell the data. So that's one way.

Another way is with something called a reverse location warrant or a geofence. And basically, what that does is it uses plot points on a map, like GPS coordinates to draw a fence around a geographical area. Now this can look like a square or rectangular, or it can look like a gerrymandered congressional district, depending on how many plots you put in the map. But imagine that the government decides that they want to draw- Let's say you live in Georgia, which outlaws abortion completely, but Florida doesn't. And there's a Planned Parenthood right across the border in northern Florida. The authorities in Georgia could set up a geofence around the Planned Parenthood in Florida, and see how many people go there and when they get the information back that identifies them, see if any of those phones have Georgia area codes, and then start investigating those people. So it's all these little data points that you generate, that can actually create what law enforcement needs to really directly target you for criminal prosecution.

Let me give a shout out for a federal bill that's out there, Ron Wyden sponsored it, called the "Fourth Amendment Is Not for Sale Act." And that contains a provision in it that says the government cannot buy your data without a court order giving them permission to do so, basically a search warrant. This is critically important because right now, the government can say, "I don't have probable cause to get a warrant against this person." These dragnet surveillance geofence warrants or reverse location where they can search for everyone who's searched for Planned Parenthood on the internet and do the same thing. Or if they can't narrow the person down that way, they'll just go and buy the data. And so you know, simple common sense laws like that, that don't allow the government to use money to get around your constitutional rights are extremely important.

You think about these reverse location warrants. If you look at Google, and again Google is just one company, it very recently released data on the reversal location warrants, and I believe it was 2018, 2019 in which they got them. These warrants are becoming a very popular police tool. And nationwide, police organizations are actually telling police departments, "Hey, are you aware how to do these things? Here's how they work. Here's how you can get them." I have seen states where the year-over-year increase in the number of these warrants was 500 percent, 1,000 percent, 2,000 percent. They've absolutely skyrocketed. The ACLU is trying to work to pass laws in states to outlaw the use of these warrants, but until we get there, you just need to be aware that Google is receiving these things, and by and large, unless the companies are selling your data, they don't want to turn your data over. But Google is not going to refuse to abide by a valid warrant. It has to do that.

So, unfortunately, I think that the best lesson for consumers is: don't count on anyone else to protect your privacy. You need to do it. You need to take the steps; you need to make the choices. I think engaging in privacy protected practices on a daily basis is the best thing to do for yourself, so you don't forget to do it when it's really important. I mean, it's kind of like shutting the ringer off on your phone all the time and then it's already off when you go into a movie theater. If somebody is going out to seek abortion care in a state where it's illegal, there's a lot of things they need to do, but better yet, adopt those practices into your daily life now, protect yourself now, and then you won't have to worry about missing a step when literally your life is on the line.

HRUSKA: We are going to get into what people can do other than going off grid. But one question I'm thinking of with Texas, where abortion is effectively banned right now. The way Texas has done this is to empower vigilantes to enforce their abortion ban. This is a notion that we're seeing other states trying to copycat. What about situations like that, where it's not the government that might be tracking your every move, it's private citizens who might be staunchly opposed to abortion and think it is their duty to go out and find people who are pursuing abortion care?

MARLOW: Unfortunately, I shouldn't say unfortunately, the Constitution protects your right to film in public. It's part of communicating and receiving information. And so, if private individuals want to go out and buy their own automatic license plate readers and sit outside of Planned Parenthood or buy their own drone with a camera and take pictures of people and then send those pictures to companies that are willing

to use facial recognition to identify people, they can go ahead and do that. And it's terrifying. So yes, if you're going to Planned Parenthood, get on a bicycle and put a ski mask over your face. This is honestly the world we're living in. Like, it's a real problem. But this is unfortunately the world that we're heading towards with abortion surveillance. There are even some states where, you know, they are using the concept of the bounty hunters and the state might actually give rewards to people. It's like- I live in New York City, for instance, anytime there's a shooting, the police put up a sign for Crimestoppers, which says they will pay $1,000 if you can, even anonymously, let the police know anything about what happened. You're going to have Crimestoppers for abortion care, where the government is going to offer people money to turn over people who are seeking abortions. I mean, it's literally a dystopian nightmare.

HRUSKA: It is. It's very 1984 So let's talk about what –

MARLOW: More like 1684, but yes.

HRUSKA: True. Let's talk about what people can do other than throwing out their smartphones and moving to very rural Maine and living without internet. What can people in their everyday lives do to protect their privacy?

MARLOW: So, there's a couple of things that I would say before going into the specifics. I'm not regularly in the habit of advising people how to commit crimes and keep it covered up. Big picture, people should keep that in mind. I am not an expert in this. I'm not an expert in telling people how to commit a crime and get away with it.

So, if you are seeking abortion care, and you're in a state that prohibits it, you need to be excessively careful. Again, just to simply be a human being with basic human rights in these states, you're going to have to be exceedingly careful. Now, when we're talking about digital privacy. There are some things that people can do that will help, but I want to again be completely clear that these things are not going to be sufficient by themselves. But, for example, if you are on the internet, and you are doing a search for reproductive rights information, there are certain search engines that are far more privacy protected than others. And the one that I would suggest to people is called DuckDuckGo. I should say, by the way, I have no commercial or invested interest in these products, and they're not endorsed by the ACLU, they just happen to work. So. if you're doing a search for Planned Parenthood, go on Google and go to DuckDuckGo, or

put DuckDuckGo into your search bar and use that as your search engine instead of Google. And it will protect the information that you're searching for.

Instead of using Google Chrome, or Internet Explorer, which are actually your web browsers, they are not the search engine, not the thing you actually type in your search to find what you're looking for, but are actually the thing that connects you to a usable internet. It is easy to track you when you use Chrome and Internet Explorer. They can track what website you go to and how long you're on it. There is a free web browser called Tor, which is spelled T-O-R, that people can again download for free. And if you use that as your web browser, it will keep secret who you are and what websites you're visiting. So that's something valuable you can do.

If you are using Google or a Google account like gmail, you need to go into your location history and turn it off and your search history and turn it off. Similarly on your phone, either completely turn off location tracking services, or you can do it by application. You can either say never track me, or only track me when I'm using the app. But then you have to be very careful when you're using the app.

Two more things I want to suggest. One, don't post anything on social media that you don't want law enforcement looking at. Even if you think it's private. I'm going to counsel people against doing that, because people can trick you. They can use fake accounts to get access to information. Don't be stupid. If you go to get abortion care in another state, and you stop off at a really good diner and love the grilled cheese, for the love of God, don't post a picture of your grilled cheese sandwich. It will have metadata in it. They can track where you are. Definitely not a good idea.

And my last one, if you're planning to travel somewhere to get abortion care, do not use a GPS app on your phone that tells you turn by turn directions. Don't even go online and put it into Google Maps and have a printout. You're going to have to go old school, the old AAA school, print out the map with nothing on it, get yourself a highlighter and map your route. It's unfortunately just what you have to do to not leave a digital trail. That being said, if you want to wear a ball cap pulled down low, put on sunglasses, do that. Now is a great time to pull out your COVID mask while you're at it. You're just gonna have to take extraordinary steps. If you are traveling in another state, pay in cash, do not use your credit card, it can be tracked. The list goes on and on, and we couldn't possibly cover them all now, but you just need to think, anytime you do

anything that is electronic, that creates any sort of digital data, you are creating a risk. And so you have towind back the clock. I mean, for God's sakes, the Supreme Court's winding back the clock to the 1950s so I guess you're gonna have to do so as well. You need to do what you have to do to keep yourself safe.

HRUSKA: This is really helpful. Two additional questions with this conversation. One, I've been talking to a lot of friends recently about preparing for a post-*Roe* world and for those of us who live in states or in the District of Columbia where abortion will remain legal even if *Roe* is overturned, the question is if a friend calls you from a state where abortion is banned, are you ready to say, "come visit me. I will help you. We will access abortion care in my state or in in DC." And so this conversation is not just relevant for the people who are accessing an abortion. It's relevant for the people who are going to be helping their friend, helping their relative, helping their child, helping their spouse access an abortion The same rules apply?

MARLOW: Yes, that's 100% right. I mean, I would certainly be even more concerned if you were a friend living in a state where it's illegal, and it doesn't even have to be the same state. If you live in Mississippi and you're helping a friend in Alabama get an abortion, Mississippi may have a law that's going to ding you in Alabama. I have seen indications that some of these states are actually looking to extend their laws across their own borders. I have real doubts that that would hold up to constitutional scrutiny. but it shouldn't be the Supreme Court that ultimately decides that. Although I think the Supreme Court is going to have to consider ramifications beyond that. What if you have a conflict of state laws, right? If New York says it's legal, and another state says it's not, whose law rules?

HRUSKA: That will be one of the next considerations to be taken up because we're absolutely seeing states trying to prohibit their residents from accessing abortion care, no matter where they access it.

MARLOW: The bottom line is, in my opinion, and I think it's the right opinion, that all of us are citizens and residents of the United States before we are citizens and residents of the state that we live in, and your rights as an American citizen, or as someone who lives or resides in the United States trump whatever limitations a state may put on it. I think states are going to try to elbow their way into being as aggressive as they can. I think they're going to try to pass a national abortion law on the federal level. All I can

say about that for certain, for absolute certain, is that the ACLU will bankrupt itself before we stop fighting laws like that. But at the end of the day, we all have to be exceedingly careful.

So, listen, if you're helping a friend from another state, what I would suggest to you is - help them. It's a basic human right, but be careful, and I would even go so far as to say this: if you're in New York, and you help someone from Alabama get an abortion, you may want to consider not visiting them in Alabama after that point. Because I don't want to see someone get off a plane and be arrested on the tarmac. You can imagine Alabama going to a company in California like Google to get information about your location in New York or New Hampshire. That's what it's looking like Your state may not even get involved. So again, when in doubt, we have to be careful. This is just the world we live in.

HRUSKA: The other issue I want to address as we talk about post-*Roe* is this natural inclination to compare post-*Roe* with pre-*Roe*. There are a lot of differences. On the plus side, people have many more options when it comes to abortion care, including abortion pills. It's easy and safe to undergo an abortion at home using an abortion pill. But there are privacy considerations even with that, where you're not traveling to a clinic but you're still leaving a digital trail. If you're ordering something through the mail, there are still privacy implications for that in a post-*Roe* world. Can we talk about that?

MARLOW: When you order online, you can't pay in cash, right? So there's a digital footprint just from ordering it. If they're going to deliver it to you, they're also gonna have to know where you live. So even if you don't provide your name, even if you write Donald Duck as your name, you're still going to have to provide some sort of address. Even if you provide a box at mailboxes.etc, mailboxes.etc has your address so that they can bill you, so there are ways to track this. I'm not even certain that certain contraceptive methods like Plan B might not be outlawed. I'll call it what it is, these nuts might go after contraception.

HRUSKA: Oh, that's absolutely going to happen.

MARLOW: Where do you even stop with this insanity. So all of these things may become challenges in the future and unfortunately, anytime you order something

online or you pay for it with a credit card, it is trackable. And that's just something you have to keep in mind. I would even tell people who think, "Oh, I'm so smart, I'll use crypto to purchase these things," crypto is far more trackable and traceable than people are letting onto or promoting.

HRUSKA: We do not have the time to talk about crypto. Oh, my goodness.

MARLOW: That's just the big picture, don't think that it is safe.

HRUSKA: Right. It's not the be all and end all. I do want to take a moment to make sure that we're not terrifying people to the point where they're afraid to access abortion care, because that, I believe, is partly what abortion opponents are hoping for. That it'll be so oppressive and so terrifying that people won't even try, that they're scared into compliance, into not accessing the care they need. After conversations like this, I am sufficiently terrified. I start thinking about how to get my tubes tied, and I get into a really, really dark place. Can we just take a moment to really underscore a point you made earlier, which is, if you need abortion care, if you need reproductive health care, you should access it.

MARLOW: Surveillance can be used as a route to identify and to punish, but what the greater cause of surveillance is, is to put people into fear. The number of people in East Germany during the Cold War who didn't even utter a word against the government because they were afraid is far more than the people who were actually prosecuted and jailed for doing so. That is part of what is at play here.

But I cannot sit here and tell someone whether they should risk their freedom in order to receive abortion care. That is a terrible and unconscionable decision that any person should be forced to make. But if it is any consolation, you can look at the data and look at the polls and know that a majority of the people in this country are behind you. They support you. They think what the Supreme Court is doing, both as a matter of policy, but even legitimacy, right? They're throwing *stare decisis* out the window. This is the only major reversal of a Supreme Court decision that I'm aware of that took away rights from tens of millions of people. It's just plain wrong. The ACLU is behind you. We will fight until literally we have not a penny left to spend to make sure that women have the right to safe and available reproductive care. We're in it with you. But at the end of the day, unfortunately, the greatest risk falls to the individual. And I would just preach

courage, because at the end of the day, you are a human with human rights. You are not an incubator, you are not a thing, and you are most definitely not, and I don't mean to offend Amy Coney Barrett, but you are not property. I don't know where her philosophies come from. But you have basic rights as a human being and probably the biggest difference, in my mind, between pre-*Roe* and post-*Roe* is for a half a century, we have known that reproductive rights are human rights. Countries that are wildly religious, like Ireland, have recognized that even with their kind of moral concerns about abortion, that women have the right to reproductive care, so the United States is moving back into the stone ages. But that doesn't mean that Americans have to, and so we just have to do the best we can.

HRUSKA: Before we wrap up. Is there legislation that can help here? You already mentioned one bill, but there have to be efforts addressing the concerns we've talked about here, right? I know that there's a broad array of legislation at the federal and state level regarding privacy broadly, but are there specific legislative efforts to address considerations about abortion surveillance in particular?

MARLOW: Yeah, so unfortunately, we're going back to the dark place. So there are, but as I've been telling a lot of my colleagues at the ACLU, there is no wall we can build to protect people if *Roe v. Wade* falls. All we can hope to do is put down as many speed bumps down as we can. And so, the laws that are out there, that we're talking about, that would protect doctors so that they can't be prosecuted in one state or for providing an abortion to people from another state. Malpractice laws, surveillance laws, like we can attempt to roll them out, but at the end of the day, the loss of *Roe v, Wade* is the loss of *Roe v. Wade*, and there's not much we can do to it.

Now, what is the good side about it? The Achilles Heel in the Supreme Court decision is that what the Supreme Court decision does is, it doesn't ban abortion. The Supreme Court decision throws it to the states to decide for themselves. So, we've been saying it at the ACLU for decades, and boy, does this phrase apply more than ever, vote like your rights depend on it. Because they do. If there are people out there who are taking away your basic rights, or the rights of your loved ones, or your friends? Vote them the hell out of office; they don't belong there. And unfortunately, it's not the most satisfying answer, but it is the most accurate one. The way to beat back this decision in the short term, until we can get a whole new Supreme Court, is to throw the people out of office who would pass laws that would take away women's reproductive rights.

HRUSKA: And on that, I just want to note, because this is one of ACS's priorities right now, when we talk about voting abortion, it applies to so many more positions on the ballot than we typically think. Secretaries of state, state attorneys general, these positions are going to have an impact on reproductive rights, whether it's state attorneys general having to decide whether to prosecute abortion bans, or whether it's Secretaries of State making sure that every eligible voter can vote and vote reproductive rights. So, when you go to your polling place, whether in the primary or in November, and you're thinking about voting reproductive rights, vote your entire ballot and remember, if *Roe* is overturned, the fate of reproductive rights goes to the states, which ultimately means state courts, and in many states, state judges are elected. Vote your whole ballot, I cannot say that enough.

MARLOW: Just to raise two other things on this point. Local prosecutors are very, very important. And there are many jurisdictions in this country that elect their sheriff. You know what, ask your sheriff, "are you going to go out and arrest people if they get abortions?" And do not vote for someone who answers "yes" to that question. I live in New York City, and we recently passed marijuana legalization, but prior to that, we had district attorneys in several of our boroughs who said, "I'm not prosecuting marijuana cases," and we had police departments saying, "we're not arresting people for using marijuana," and that was the end of it. So yeah, you've got to get out and vote wherever you can, and you've got to rely on people to make an impact wherever they are.

HRUSKA: Last question. When it comes to privacy, I'm always looking to the EU. They're always ahead of us on privacy. And while there the abortion situation in Europe is vastly different than it is here, is there anything to be learned from what the EU is doing on privacy because they are going after Big Tech in a way that's almost inconceivable here in the States.

MARLOW: The big lesson we can take from the EU is that by passing a comprehensive consumer privacy law, they have prevented, not completely but to far greater degrees, individuals' data from ending up in the hands of companies and data brokers who could then sell it to others. It's almost like the concept of an attractive nuisance, right? Because we have failed to pass a similar law in the United States. Now that *Roe v Wade* is going to be overturned. We have all that data sitting there. We have companies that

have developed entirely around the concept of surveilling people, collecting their data, and making it available to private parties and government entities. That all happened. That marketplace happened, and the risk is growing because we do not have stronger privacy protections in this country. Again, even if we passed an EU-style privacy law, it would be just another speed bump, but the more speed bumps we throw in the way, the tougher it becomes for people to go after those who are seeking reproductive and abortion care. That just simply is the best we can do until we get our hands around creating a better, fairer and more legitimate Supreme Court, which is a conversation for another time,

HRUSKA: And which we talk about often on this podcast.

MARLOW: I bet you do.

HRUSKA: Thank you, Chad, so much for this conversation. I will say I am sufficiently paranoid after this conversation, but I really appreciate all of the steps that you recommended people take. It can feel extreme. This conversation can feel hyperbolic. It's not. This is the world that we are about to enter, and privacy needs to be something that we start thinking about each and every day, if not each and every hour, given how much of our lives are lived online.

MARLOW: Thank you so much for having me. I appreciate it all. You know we can all take off our tinfoil hats now, but the rest of the things we discussed - best to get to them.

HRUSKA: Thank you, Chad.

And thanks to our listeners for finding Broken Law. You can help us reach more listeners by recommending Broken Law to a friend, and please be sure to follow and subscribe, so you don't miss an episode.

If you have ideas for future episodes, please let us know. You can email us at podcast@acslaw.org. Or find us on social media @acslaw.

Together, we'll speak truth to power about the law, whose interests it really serves, and whose it does not