wiley

FBI Lockbit Takedown: What Does It Mean for Your Company?

Wiley Connected
March 1, 2024

Wiley's Privacy, Cyber & Data Governance team looks at the recent takedown of the "Lockbit" ransomware group. Join Megan Brown, Lyn Brown, and Josh Waldman as they discuss how the government went after this prolific and dangerous ransomware crew, what companies can do to protect their systems and data, and how the FBI works with companies both before and after a ransomware incident.

Transcript

Intro

You're listening to Wiley Connected, a series of podcasts on tech, law, and policy. In each podcast, technology focused lawyers at Wiley, a Washington, DC law firm, break down innovation and law with a uniquely DC perspective.

Megan Brown

Welcome to Wiley Connected, I'm Megan Brown, Co-chair of Wiley Rein's Privacy, Cyber and Data Governance Practice, and I'm joined today by Lyn Brown, who is Of Counsel in our practice and Josh Waldman, who's an Associate, both of whom had extensive backgrounds at the Federal Bureau of Investigation, and with me, help manage all kinds of cybersecurity issues. Today, we are getting together to talk about ransomware, and in particular, a significant enforcement action that was taken last week. The U.S. and U.K. governments, together with other international law enforcement agencies, made some major announcements spread out over several

Related Professionals

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Privacy, Cyber & Data Governance

hours and days about criminal indictments and sanctions and activities against members of the LockBit ransomware group. This takedown presents an opportunity to better understand how the U.S. government is addressing ransomware, how companies can prepare for ransomware and how to work with the government, if you are the victim of ransomware. Josh and Lyn spent lots of time at the FBI and help clients deal with these issues regularly. I wanted to get Lyn and Josh together to share their perspectives on the takedown, and put it into context. Thank you, Lyn and Josh for joining me.

Josh Waldman

I'm excited to do this.

Lyn Brown

Happy to be here.

Megan Brown

Let's table set. Josh, why don't you give us a little primer on what ransomware is and why it's considered such a huge cyber threat?

Josh Waldman

Thanks Megan. Well, the cybersecurity infrastructure security agency are CISA, they have a definition of ransomware. They say it's "ever evolving form of malware, that's designed to encrypt files on a device. It renders those files and the system that rely on them unusable." And then what you'll see is the malicious hackers will then demand ransom in exchange for decrypting those files. Basically, they lock up the stuff on your computer, and if you don't pay, you can't use what's on it. We've seen that these ransomware hackers can be prolific. This indictment that was announced on February 20th, and the U.S. Department of Justice, DOJ, they say that this LockBit group deployed their ransomware against more than 2,000 victims in the U.S. and around the world, and that means hundreds of millions of dollars in ransom payments, and the indictment alleges that LockBit received over $120 million in ransom payments over the past few years.

Lyn Brown

Another notable, but not unique feature of the LockBit group is its federated structure, with skilled hackers, termed developers or administrators creating ransomware as a service offering. This basically lets anyone who is willing to pay termed affiliates, have the ability to deploy and manage ransomware attacks against victims of the affiliates choosing. LockBit even went so far as to offer a dashboard or control panel for its affiliates to help them facilitate their crimes.

Megan Brown

Lyn let's unpack that for listeners. We've heard of software as a service, infrastructure as a service, and now unfortunately we have ransomware as a service. What did that actually look like here?

Lyn Brown

Well, much of the LockBit infrastructure was hosted on the dark web. Once a new affiliate joined the LockBit ransomware conspiracy, the affiliate was given their own control panel, hosted at a unique domain name on the dark web. The affiliates would then gain unauthorized access to vulnerable computer systems through, for example, hacking or network penetration techniques were using stolen access credentials purchased frequently from third parties. The affiliates would then deploy LockBit within the victim computers systems, which would allow them to exfiltrate documents and data on the victim computer systems to encrypt the data on the victim systems, and then they would leave a ransom note that provides the victim with instructions on how to contact the affiliate, and they would threaten to share publicly the victim's stolen data and leave the victim's data unencrypted and inaccessible to the victim.

Josh Waldman

I think what is interesting here, is these indictments provided a lot of detail into how the LockBit ecosystem works, right? The facts here show that the ransomware incidents can be really harmful and dangerous. For example, in recent months where we've ransomware incidents disrupt the hospitals in the U.S., and that makes it really hard for the day to day, for the medical professionals, dangerous for patients. We've also seen reported ransomware incidents at major companies in the last year that has disrupted production and operations, and they can cost hundreds of millions of dollars to companies that are affected by these ransomware attacks.

Megan Brown

I really appreciate the background and the level set. Obviously, we've worked together on ransomware, both attacks and policy issues, I'm curious if you could help us understand what the government and its partners here, actually did. What did this takedown entail? What are they saying publicly, I guess, that's sort of an important limitation.

Lyn Brown

We know from the press conference and the related press release, and the unsealed indictment that the FBI and DOJ took a variety of actions. First, they coordinated with their international partners to seize the public facing websites and servers that were used to command LockBit ransomware. These seizures disrupted the ability of LockBit hackers to attack and encrypt networks and extort victims by threatening to publish stolen data. The U.S. and U.K. authorities actually placed a notice on LockBit's victim shaming website that the site is now under the control of the U.S., the U.K., and the Kronos Task Force. The C site now reportedly also offers free recovery tools and news about the arrest of LockBit affiliates.

Josh Waldman

Yeah Lyn, I see it has, the seizure is trying to stop LockBit from doing this to more people. Like you said, you know for those that are already victimized, part of this announcement was that the U.K., International Crime Agency working with the FBI and other international law enforcement partners, they actually did all the decryption capabilities for some of the LockBit ransomware. As you said, there's that notice now on what used to be the kind of LockBit homepage, right? That victims in the U.S. can contact the FBI, and FBI and DOJ made this special website just for victims, that you can go there and contact the FBI and they might actually be able to decrypt your files without you having to pay ransom to the criminals who encrypted them. Those are sort of two coordinated actions taken together. Takedown of the after infrastructure, and then a tool to help folks who've already been victimized. One of the takeaways from this, is it shows, first of all that the LockBit ransomware threat was global, it affected people around the world. But I think it also shows that the U.S. and the U.K. had that very close collaboration and other international partners in there as well, to go after this significant crime operation they really had to have international law enforcement cooperation to get it done.

Megan Brown

Lyn, having been at the FBI for as long as you were and sort of seeing similar types of activities and initiatives for a long time, what do you find significant about this?

Lyn Brown

Well, I think what's significant here is the nature of the joint operation to take down, what was a prolific and destructive ransomware group that was literally operating throughout the world. LockBit members had executed attacks against thousands of victims in the U.S. and throughout the world for the last 4 to 5 years. I think the other significant thing about this, is the amount of international cooperation necessary. This had to be a very real coordinated approach to take down 34 servers or so throughout the Europe, Australia, and the United States. That's a lot of effort by a lot of people to effectuate this takedown.

Megan Brown

Did they actually go after the bad guys? In the past, when we've seen sort of indictments in absentia, I think DOJ has faced some criticism because some cynics will say, like that's a waste of time, the criminals are overseas, they're beyond our reach, but here, what did they do to target the actual bad guys as well, beyond taking down the sites and seizing assets and domains?

Lyn Brown

Well, that's a good point. In addition to taking down the infrastructure and developing a decryption capability that they're able to share with victim companies, DOJ unsealed the indictment that was against the two individuals listed, both Russians, for being part of a global conspiracy to deploy this ransomware variant. As we mentioned at the top, the LockBit has been around for a number of years, and it's been deployed against more than 2,000 victims since around January of 2020, causing more than $120 million in ransom payments.

The two criminal defendants here were part of a global conspiracy, not only to enrich themselves and others by developing the LockBit ransomware variant, but also by maintaining the LockBit infrastructuring of the computer servers and the affiliate control panels, etc., and hacking into and deploying LockBit against victim computer systems.

Josh Waldman

And Megan, I think to follow up on your question about, are these indictments effective? I think it's two pieces there to think about. One is the level of detail in this indictment, there is some deterrent effect to explaining how this system works. The ransomware is sort of a closed ecosystem, not just anyone can understand how it works, thankfully if you haven't been victimized, so by putting all that out there, I think that does hit the criminals a little bit. Then the other piece that comes into this is, in addition in the indictment, you now have the Treasury Department sanctioning these two Russian hackers, and that hits somewhere they care about, which is the wallet. At the end of the day, most of ransomware hackers, are doing this to make money, right? If you pay a ransom, they make money. When Treasury issue sanctions against the indicted individuals, it does start to bite back at their ability to make money off of this, and I think what we've started to see from the Government, over the past couple of years, is this coordinated set of actions against ransomware. You're taking down the infrastructure they used to commit the attacks, the decryption capability, indictments and now financial sanctions, that's becoming the playbook that the Government is using against these most impactful ransomware hackers. The ones like the two named in this indictment, that develop and distribute these widely used ransomware variants. We've seen a couple of times before, like in January 2023, DOJ had a similar announcement, taking down a ransomware group called Hive, and then a few months later in May, there was a sanctions announcement against the Russian national who had help developed the Hive, and actually the LockBit ransomware that was addressed on last week. The other piece of the financial activity is, at times the government actually been able to recover ransom payments, it's usually from cryptocurrency accounts that the hackers use to collect ransom and move money. In addition to certainly understand the criticism that somebody who stays in Russia may not end up in jail anytime soon, the government respond to that, in two ways. I think one would say, well look, some of these folks do like to travel around the world, and by having international partners, you may be able to arrest and extradite them, we've seen that happen a few times. Then secondly, by cutting off and going after the financial network that supports them, that can really eat away at their ability to make money doing this, and maybe they'll go into another line of business.

Megan Brown

Thanks Josh, for all of that. It is great to see the takedown and the cyber community was very pleased, particularly Lyn, with the screenshots of the seizures of the websites. I think people thought that was really nice to see, and we're very heartened by the progress that you guys have just described. I do want to shift gears a little bit and think about what this might mean for companies as a practical matter, right? You see this in the news, and I think organizations in the private sector may wonder kind of, what does this mean for me? What lessons can I take from it?

Lyn Brown

Sure. So as significant as this takedown is, there really are several things that companies should take away from this. First, is that ransomware isn't going away just because the LockBit variant is now disrupted. These type of threat hackers unfortunately are relatively resilient, and with the monetary payments out there, they're not likely to cease anytime soon. Because there's still a threat out there, organizations need to prepare for, continue to guard against ransomware incidents. As this week's announcement shows, the government does have capabilities like decryption tools that can help companies victimized by ransomware. We certainly recommend, that companies engage with the government if they do experience a ransomware incident.

Megan Brown

Let's dig in, a little bit more to this preparation piece. We advise companies and organizations on all kinds of incident preparedness, but over the past couple of years that has grown to include more specific work targeting ransomware threat and understanding both how ransomware might affect an organization, what the bad actors might be seeking to do, but also how to get ready for it, and be able to respond to it. So, Lyn let's talk a little bit about that preparedness piece of it.

Lyn Brown

What we see, and certainly you're right advise companies on, is that there's going to be a mixture of technical and policy or process issues that they need to think about. NIST has put out Guidance, CISA has a Stop Ransomware Guide, the FBI has a variety of products and those are helpful tools for companies to use to think about cyber hygiene and technical measures, and how to help secure their systems. The various government products are instructive, and they can again help companies that are developing robust programs to anticipate and address ransomware threats in particular. Companies need to think about having a cyber incident response plan and they need to practice it regularly. Practice is an important, but frequently overlooked part of preparation, so have the tabletop exercise to see how the incident response plan works and practice before you're confronted with an actual incident. Companies need to do that tabletop exercise with their senior leaders, the CISOs, the general counsel, and other stakeholders, to see where the gaps in their response may be. Any cyber incident, but particularly a ransomware incident, is going to create disruptions, going to create stress. It's unfortunately not uncommon for some ransomware hackers to harass or even threaten a victim, companies' employees, to try and speed up a ransom payment, so again, be prepared. It can help minimize the stress if roles are articulated and practiced in advance. I think it's also important to remember that a victim company or organization may lose access to critical systems or files during a cyber incident, and may not be able to process payments, let's say, or track shipments and customers may start calling or may get concerned about being able to contact a company in a cyber incident. So it's important to anticipate those kinds of impacts and potentially have alternate methods of communication set up in advance. Again, anticipating and being ready for these types of things is really key.

Megan Brown

Let's talk a little bit more about another aspect of preparedness, because I think all the stuff you just went through is really smart and kind of table stakes to be ready for an incident, but there's another piece of preparedness that we've seen as a big differentiator, and that's resilience and redundancy, right? Having backups and having the ability to restore data and systems. Why's that important?

Lyn Brown

Well, it's important for a couple of reasons. It helps companies assess the damage. It helps them to be able to get back up and running, if they have backup systems in place, it also helps them with a potential ransomware payment decision. Maybe they don't need the encryption keys if they're able to get their systems back online on their own, but again, conversely, if they don't have adequate backup systems, and they make a business decision that they need the data sooner rather than later, they may seek to pay the ransom. It all goes to the pay or don't pay decision that needs to be made by these companies if they suffer a ransomware attack.

Megan Brown

Those decisions are hard and, maybe we'll touch on that in a little bit, on kind of the tradeoff and thinking there. Josh, we haven't chatted with you in a second. Regardless of a payment decision, although payment certainly can affect some of these things, what are the government obligations that are triggered by a ransomware event that no doubt some of the victims of LockBit had to confront?

Josh Waldman

Yeah, thanks Megan. I think, we see that companies have to respond when they have a ransomware incident and make disclosures to the government. For example, the Securities and Exchange Commission, companies that are registered with them, there are new rules for reporting cybersecurity incidents publicly, and then for other companies, that might be regulated by a sector specific regulator, such as the Transportation Security Administration or the Federal Communications Commission or state regulators, they're going to have obligations to notify those regulators about the incident. Then also if you're a federal government contractor, they're reporting requirements about cyber incidents that could be triggered when a ransomware incident affects your company. You got to remember too, some of these reporting obligations come up fast within 72 hours, for example, to the relevant Department of Defense office right now. TSA, Transportation, Security Administration, they're looking at 24 hours for pipeline and surface transportation. Those obligations are going to be on top of your company's efforts to respond to this incident and get things back up and running. Inside that pressurized environment, we're seeing more and more that ransomware hackers understand that, and they're trying to take advantage of that pressure. They might use publicity to exert pressure on the victim company, their goal there is to drive that payment decision, and we'll talk a little bit more about that, right? But again, they want that company to decide to pay ransom. Interestingly, threat analysts are seeing more and more often than other forms of cybercrime-based extortion are happening a lot, where they don't actually encrypt the files, but the hackers are just using that public pressure or harassment, threatening to release

data, showing that your company got hacked, in order to go the company into paying.

Megan Brown

No, all those pressures are really hard and make it challenging for victims, as you said Josh. One thing that I think, companies also need to keep in mind and just sort of be aware of, is part of the preparedness that Lyn described is, do you have cyber insurance? what does it cover? and how can say your broker or your insurer, help you. Insurance policies can cover and include forensic support, as well as ransomware negotiation support.

Josh Waldman

Megan, it's a really good point. We have an actual ransomware incident, as opposed to some other type of cyber security incident. There are specialist capabilities that a company is going to want to consider having access to, and when you want to have access to them, you want to make sure you get that set up in advance. Somethings to think about with ransomware, that you might need a specialty provider on, are if you're considering making a payment, well, how do you actually do that? how do you actually make the payment? There are specialist negotiator services who deal with ransomware hackers who has specialized in that negotiation and helping walk companies through ransomware specifically, they're going to work with an existing cybersecurity services firm and an existing legal counsel. You're also going to want to think through, if you're a victim company of one of these ransomware incidents, is kind of what's your process on assessing and deciding whether to pay ransom?

Megan Brown

I think that's a great pivot Josh, to this question about the payment decision. Paying ransom is controversial, it has been the subject of a lot of debate. When we saw, for example, after the Colonial Pipeline incident, the CEO was pulled up before Congress, and I think people, some people criticize the decision to pay, others thought it was prudent in light of the full circumstances. I think let's chat about, kind of Lyn, where's the government on this now?

Lyn Brown

There's a general sentiment in the government of discouraging ransom payments. The reality is that, paying a ransom doesn't necessarily guarantee that a victim's files are going to be recovered or that the decryption tools that are provided are going to work or that they're even going to be provided, in the first place. The FBI and CISA discourage paying, but the FBI said it recognizes that at the end of the day, this is a business decision. Treasury has been more vocal about advocating for banning ransom payments. I think the White House actually considered doing just that, sometime last year. Some states are taking a look at the issue, North Carolina and Florida, for instance, have made it illegal for state and local agencies to make ransom payments. There is some movement, at least at the state level, toward banning payments. There are significant legal risks about making a ransom payment, I think companies need to be aware of. First and foremost is the potential for violating sanctions. In the LockBit takedown, Treasury move quickly to add the two

indicted Russians to the sanctions list, there's a mechanism there for going after the criminal defendants and we're hearing more, and more, influential voices that are advocating for banning ransom payments in their entirety. There's a thought that these payments facilitate and encourage ransomware attacks, and that if you ban the payments, then you'll discourage the commission of this crime. Not sure how accurate that is, but that's the thought process at least.

Megan Brown

Lyn, I appreciate all that. We've worked with clients on some of these attacks, and I'm curious for you guys to share some of the lessons we've learned about the considerations that go into making payments.

Josh Waldman

Yeah, absolutely, because as Lyn said, well, it is ultimately a business decision right now. You can pay ransom if your company decides that's the most appropriate business decision in this circumstance, given obviously doing some other checks, and we'll talk about some of the specific things that you might need to do, but when your company is experiencing a significant disruption, and there's a potential to alleviate that, you're going to have to consider paying. Some certainly will consider paying. A payment decision is going to have to look at a lot of factors, besides a sanctions check, about where your money might actually go, you've got to take a look at what systems and data are being affected by the incident? How critical are those to your operations? What's a timeline for getting them back up and running? Do you have backups? As you talked about earlier Megan. And then you also want to get some insight into the capabilities and the history of the threat hacker. As Lyn you said, not all of these ransomware group will actually decrypt your stuff, so you're going want to know as much as you can about the threat hacker, before you try to make that decision.

Lyn Brown

I think that goes to the issue of the pay or don't pay decision that these companies have to make. You're talking to the FBI and establishing that dialogue and learning what history they have with some of these threat groups can really be important. We've certainly found in some of the cases that we've had Megan, that the FBI can provide important insights into the threat hackers negotiation strategies, into their tactics, whether they have been reliable, and actually providing decryption keys or whether they are unreliable, and even if a company pays, they still go and leak the data. Having that awareness and leveraging the threat information, threat actor information that the FBI can share with victim companies, becomes really important in having a company be fully informed when it makes a ransomware payment decision. It's also possible that the FBI may have already developed decryption tools on its own, or in coordination with other seizures from other ransomware groups, and may be able to provide those decryption tools to the victim company for free and then there's no need to pay the ransom.

Megan Brown

We've worked with the FBI on these issues, and I will say, I'm sure you guys agree, the FBI has really done a nice job over the past decade of kind of transitioning its rhetoric and making sure that victim companies feel like the FBI is a willing partner, and has their back, so to speak, but for companies and listeners who may have never interacted with the FBI, what do organizations need to think about if they are considering, picking up the phone and calling their local FBI agent?

Lyn Brown

Well, I think a couple of things. One, I think, do so before the incident, but certainly consider contacting the FBI if you're in the middle of a ransomware attack or a cyber incident, but it's important, as part of the preparation piece to get to know who will be the responders to a cyber incident if you have one. Have your local FBI contacts in the relevant field offices established beforehand so you know who to call if you suffer an incident and have that dialogue, know the people that you're dealing with ahead. It makes the incidents, although they're always stressful, perhaps a little bit less stressful if you're actually dealing with cyber agents that you've met and talked to before. The FBI has 56 field offices in the U.S. and multiple smaller offices across the country. There's an FBI office that's close, usually to wherever a company operates, and someone can be made available to respond to an incident or to come out and get to know the General Counsel and the CISO beforehand, as part of incident response preparation. We've helped companies contact and coordinate with the FBI during a ransomware incident, and we've also helped build those relationships in advance too. Again, it can be really helpful in the pressurized environment of an actual cyber incident, to be calling someone you've met before, and who has a general understanding of the nature of your business and your organization and is there to help.

Megan Brown

Then what should organizations expect if they do report a ransomware event to the FBI?

Lyn Brown

They can report to the local field office, or they can report through online through IC3.gov. I think what they can expect, is that they'll be contacted by an agent from one of the local field offices who work in coordination with whatever field office has a lead for that particular ransomware group, and there'll be a continued dialogue, I think, between the victim company and the FBI about the nature of what the victim company has experienced. And if there's indicia what ransomware group may be involved, and then that goes back to what we talked about earlier in terms of the information the FBI can provide about that threat hacker history, their history of providing decryption tools upon payment, their history of being reliable, using air quotes there, being reliable in terms of doing what they say they're going to do, again with respect to providing decryption tools or otherwise keeping this confidential. I think that those are some of the expectations that companies can have.

Josh Waldman

Then in terms of what you're actually going to see, when you are working with these companies, and one of the reasons we recommend kind of reaching out to the local field office, and Megan talked about kind of how there's been this shift in the last decade or so, the FBI agents and supervisors, and the analysts, and the computer scientists who work in the cyber squads, it is part of their job now to build relationships with private sector companies in their area of operations. When your company is potentially victimized, we reach out to your local field office contact, know they're really going to be your point of contact to kind of interface with that broader FBI organization that may swing into action to potentially help or investigate, they might have to coordinate with another FBI field office. A lot of companies have operations in multiple states, multiple locations. They might want to review a sample of the malware that is affecting your company in the ransomware incident. These things that they can do, hopefully they're going to, we've seen it, certainly in instance that we worked, they've tried to kind of limit the friction of sort of two large organizations coming together and not appearing coordinated. It's brought to the broader government policy and to the FBI operating procedure, to try to present a unified face to the company victim and do what they can to help out.

Megan Brown

But aren't companies reasonably worried about being publicly exposed? I mean, I would think companies are wary of that risk.

Lyn Brown

I think that's right, but if you look at the LockBit indictment, for example, I think it shows how the FBI has really tried to be discreet and not revictimize victims, as they say, and the LockBit indictment does not name the individual victim organization, the companies are instead described in a more generic fashion. Victim one, a law enforcement agency in New Jersey, or victim two, a business in Minnesota. In other words, the exact names of the organizations or companies that were victimized were not publicly disclosed. Again, to the FBI, that's an important part of its goal, not to revictimize the victim of a cyber-attack.

Josh Waldman

I'll just add here it's something that the Bureau said a couple of times publicly, is they like to say that, if you're the victim of a cyber incident, they're not going to show up at your door, with those blue FBI ray jackets and lights and sirens, they're going to be discreet. They're going to work with you and it's going to look like any other vendor, or consultant, or supplier is coming to your door to help out.

Megan Brown

As we wrap up, this area is getting a ton of attention, rightly so, this is a busy week of developments, and I just wanted you guys to share kind of, your top final takeaways from the LockBit takedown.

Josh Waldman

Well, I think on the government side, it shows that they're clearly making some progress in combating the ransomware threat. This takedown shows that there are strong international commitments to working together, to dismantle these kinds of cybercrime operations, and to help protect companies and citizens, not just in the U.S. but around the world.

Lyn Brown

I agree. This type of coordinated effort and announcement takes a tremendous amount of interagency effort and international cooperation, especially to get the sequencing right. There are a variety of different agencies that need to work together, often under tight timeframes or challenging circumstances to do a global takedown of this size and scale. I think it's really a remarkable accomplishment.

Josh Waldman

I mean, I think that said, right, that's the good news, the bad news is there's a lot of ransomwares out there still and companies do still need to be prepared for it to impact their operations. This one LockBit takedown, while its impressive and hopefully impactful, it doesn't get rid of ransomware everywhere.

Lyn Brown

There are a variety of things that companies can do to be prepared for a cyber incident, many of which we've already talked about, but we recommend working with counsel to develop and practice a cyber incident response plan that includes ransomware considerations and build relationships with the FBI in advance. They can often provide actionable information for ransomware response, and it's going to be a lot easier if you know the right folks at the FBI to contact and work with before a cyber incident occurs. There's simply is nothing better than preparation. Have a cyber incident response plan, know who to contact, have your cyber vendors lined up in advance, and do your tabletop exercises regularly, try and stay ahead of these emerging types of cyber threats.

Megan Brown

Thanks Josh and Lyn, for taking the time to unpack some of this. We hope you'll join us for the future episodes here on Wiley Connected, where we'll talk privacy, cyber and other current events. Thanks, Lyn and Josh.

Lyn Brown

Thank you.

Outro

Thank you for tuning in to the Wiley Connected podcast brought to you by the attorneys at Wiley. If you enjoyed this episode of Wiley Connected, we encourage you to subscribe, rate, and leave a review on iTunes and SoundCloud. For additional resources and materials, head over to wileyconnect.com. Thank you for listening.

The views, information, or opinions expressed during the series are solely those of the individuals involved and do not necessarily represent those of Wiley Rein LLP and its employees. The material contained in this podcast is not intended to be and is not considered to be legal advice. Transmission is not intended to create and receipt does not establish an attorney client relationship.