

INTERVIEW :

IF IT WERE A RACE, DEEPFAKES WOULD BE MILES AHEAD OF THE LAW

Karen Painter Randall knows that it's hard for lawyers to keep up with cybersecurity. A partner at the law firm Connell Foley, where she chairs the cybersecurity, data privacy and incident response group, Randall said it can be hard for anyone to keep up. She sometimes tells associates at her firm, "If you're not reading up on the developments in this space on a daily basis, you're two weeks behind." Even so, she was surprised at the response she got in October when she spoke at a conference at a large law firm. "Does anyone know what deepfakes are?" she asked, referring to images, videos and audios that are manipulated to make it appear people are saying or doing things they didn't say or do. The response was silence. "No one knew what they were," she said. But that's about to change, Randall predicted. "It's not that deepfakes are coming," she said. "They are here, and they're following the footsteps of the cyberattacks we've seen over many years now." Randall talked about recent legislation designed to offer protection in a handful of states, but it's unclear how effective these laws will be. Among her suggestions: This could be a good time to check your insurance.



Karen Painter Randall

TAG Cyber: Are all deepfakes harmful?

KAREN RANDALL: No. If you remember the British soccer star David Beckham, he had a campaign that he was working on for malaria awareness, and they took his voice and they **used it in eight foreign languages**. When you saw the commercial, it looked like he was really speaking the languages. Another example I like to use is Val Kilmer. As you know, he was one of the "Top Gun" movie stars back in 2015. After that movie, he was diagnosed with throat cancer. His treatment drastically altered his voice and threatened his acting career. **Deepfake technology** allowed him to overcome this setback and perform in the 2022 movie "Top Gun: Maverick." So deepfakes can actually be beneficial.

TAG Cyber: What are some ways that deepfakes are particularly dangerous?

RANDALL: Well, I always like to use a Putin quote that I heard many years ago, before we really started to talk about deepfakes. Putin was quoted as saying that whoever becomes a leader in artificial intelligence will become the leader of the world. And artificial intelligence is what is used to create these deepfakes. A good example of what Putin may have



Deepfake technology helped Val Kilmer.

State laws have criminalized the distribution of nonconsensual deepfake pornography and deepfake attacks on political candidates.

meant was a deepfake video released last March of Volodymyr Zelensky instructing his troops to stand down and to surrender to Russia three weeks after the invasion. Fortunately, they were able to catch that video, Zelensky denounced it as fake, and nothing happened as a result. But that is very significant in terms of how people can use some of these deepfakes.

TAG Cyber: Let's talk about damage that deepfakes can do to companies.

RANDALL: For corporate leaders and key stakeholders, like board members, you can try to shame them, put words in their mouths that they never used. That could have an impact on the value and brand of the company. For marketing purposes, people may not trust what the company is doing. For public companies, you may see stock prices drop. And then certainly you worry about cyberattacks on companies. Some of the cyberattacks that we see today include business email compromise attacks where the attacker hacks into an email, sets up rules and tries to pretend that they're an executive to steal information or to misdirect funds. But in this case, they don't even need to send an email. All they need to do is use an audio deepfake that sounds legitimate. Call someone who's in charge of the funds, pretend that they're the CEO of the company and tell them that they need to change the direct deposit instructions so that deposits go to Bank B instead of Bank A. It actually happened to the **CEO of a U.K.-based energy company**. He got a call from the man he thought was the head of the firm's German parent company telling him to change the direct deposit to a Hungarian bank. He lost approximately \$250,000 in doing that. And keep in mind, with some of these public companies, they're on the internet all the time. They're giving public speeches, they're giving webinars, they're teaching, things are being recorded. Both their pictures and their audio are very easy to get to be used to create deepfakes. I think you're going to see more and more of that.

TAG Cyber: How about the threats to the public interest? What are the kinds of deepfakes that should concern us all because they could affect us all?

RANDALL: Some of the laws that we'll discuss have certain focuses. Some just focus on pornography, some focus on elections. If we're seeing more and more political deepfakes, they could erode the public trust in government and news. I think we're probably getting close to that. There could be difficulty discerning the difference between what's true and what's false. I think it could threaten democracy if it's used for propaganda by some of these state actors and certainly in campaigns. And I think it creates geopolitical competition to be the best in this area. But I want to read you a quote that I came across that really applies. **Hannah Arendt** was a political theorist, author and Holocaust survivor. "People who no longer believe anything cannot make up their mind," she said. "They are deprived of the

capacity to think or judge, and with such people, you can then do what you choose.” I thought that was particularly applicable to what we’re talking about today, especially with regard to what impact it has on the public interest.

TAG Cyber: Recently, there have been attempts to pass laws specifically to combat deepfakes. Can you tell us about them?

RANDALL: When you say laws that could be used to “combat deepfakes,” we came across no case law at all with regard to combatting deepfakes. But as you know, there are certainly tort and civil suits that could be used. Intellectual property law could be used. And in the last few years, a few states did pass **deepfake legislation**. The state law examples start with Virginia. In March 2019, Virginia became the first state in the nation to impose criminal penalties for the distribution of nonconsensual deepfake pornography. It made the distribution of the material punishable for up to a year in jail and a fine of \$2,500. It was considered a misdemeanor. It’s probably because a lot of these




Deepfake of Obama (l) and Jordan Peele, who created it

deepfakes do involve pornography that they wanted to address it upfront. Then that was followed by Texas in June 2019. It became the first state to prohibit the creation and distribution of deepfake videos intended to harm candidates for public office or influence elections. And the Texas law defines a deepfake video as a video created with the intent to deceive, that appears to depict a

real person performing an action that did not occur in reality. So they focused on elections. And I think we’re going to see more and more of that.

There are many deepfakes of former presidents and other state and global leaders. Filmmaker Jordan Peele made a **deepfake of President Obama** criticizing President Trump. So again, just like the Zelensky deepfake, some of these could have a huge impact on global stability. California enacted two laws in October 2019. One allows victims of nonconsensual deepfake pornography to sue for damages, another provides candidates for public office the ability to sue individuals or organizations that distribute election-related deepfakes without warning labels near election day. So now we’re evolving to the point that they want you to put warning labels on the deepfakes, probably trying to get around the First Amendment argument that they are protected speech. As far as federal law, there have been a lot of bills introduced, and so far they have all failed.

Check your cyberliability policy for deepfake coverage, but be sure you understand everything it covers and excludes.



TAG Cyber: You were talking about a variety of new laws, but what about defamation laws? And what about fraud laws? Could these not be used by victims of deepfakes to try to find justice and force the perpetrators to pay a penalty?

RANDALL: Absolutely. I think there's all sorts of civil suits that could be brought: invasion of privacy is another suit that could be brought, but I think the waters are being tested. As I mentioned, I haven't seen any case law out there that addresses these types of claims involving deepfakes, but I think you're going to see a lot of them. There are issues in proofs with regard to some of those claims.

TAG Cyber: I wouldn't think these state laws are going to be easy to prosecute. They're resource-intensive to do an investigation, to bring charges. And, as you say, they're new and untested.

RANDALL: Yes. You have to gather your evidence. And I think that's going to be one of the key issues. I mean, the same applies for data breach litigation. But these are a little different. With the data breach litigation, our forensics team is able to, in a lot of cases, find the root cause of the incident. For ransomware attacks they're able to identify the ransomware group that was responsible. Getting those proofs together is a lot easier than deepfakes because you don't know who's behind a deepfake. It's very difficult to track. They're anonymous. You're going to need law enforcement involved, as you mentioned. You're going to need the digital forensic team, you're going to need a media manipulation company, it's going to be very costly. And what's going to be interesting is whether or not insurance is going to cover a cyberattack that involves a deepfake. That's transferring that risk to a policy. It's going to be interesting to watch.

TAG Cyber: So how do you suggest that companies and individuals, but especially companies, prepare themselves and deal with these threats, these risks?

RANDALL: Just like they do any other type of business risk. I mean, cybersecurity is the number one business risk for companies. Obviously, that impacts the consumers, the employees, the people they do business with, their third-party vendors. So just add deepfake onto that right now. We are educating people on cyberattacks. different types of cyberattacks out there. What the threat landscape is. There is a lot of collaboration with law enforcement. As I mentioned earlier, the FBI rolls out advisories. They actually rolled out an advisory on deepfakes telling people that if you're interviewing people remotely, you better be careful about it. Some job candidates are turning out to be deepfakes. So now everyone is on notice that they better be careful.

And then, I've got to say, a lot of people forget that being prepared includes having that incident response plan in place—and practicing those plans, having tabletop exercises. Again,



A David Beckham deepfake allowed him to warn people about malaria in multiple languages he could not speak himself.

put a deepfake into it. I just did one with a major health insurance company. We put a deepfake into the exercise, and it was very helpful. Imagine having a cyberattack involving deepfakes. What are you going to do? You're not going to know which end is up. You don't know who to call, you don't know how to document that evidence. And that's going to have an impact on the outcome of your response effort.

TAG Cyber: I know you do a lot of work with insurance companies that insure cybersecurity events. How do they view deepfakes? Is this just part of the same environment? Or are they looking at this as a different or a new kind of risk?

RANDALL: I think they're aware of the risk, and they're digesting the impact the risk may have on the insurance market. But I have not had a case with any insurance carrier that involved a deepfake. And as you know, every cyber insurance policy is different. So it'll be interesting to see how they underwrite that risk. I don't know if they've already done that. But that might be a good discussion for us to have later—maybe bring in someone from the insurance industry and talk about how to evaluate this.

TAG Cyber: Would you advise your clients to take a look at their policies, and decide whether it looks like it covers deepfakes, or have a conversation with their insurers and ask them to add language that makes it clear?

RANDALL: I would recommend that they have a policy in place that would cover any type of cyberattack that involves deepfakes. Certainly start with your broker if you're going out to market for a cyberliability policy. Start the discussion with the broker and let them know that this is something that you want to make sure is covered in the policy that they recommend. And then understand your policy. A lot of people get a cyberliability policy, but they don't know what the coverages are, they don't know exclusions, they don't know sublimits. So I highly recommend that when they're doing this as it applies to deepfakes, that they also make sure that they understand the nature and scope of their policy.

