Proskauer

Transcript:

Privacy on the Web

Kristen Mathews – Head of Proskauer's Privacy & Data Security Group

S. Mazyck: Hello, everybody, on this Tuesday, May 10th. I'm Spencer Mazyck, and this is the Bloomberg Law Podcast, a series of interviews focusing on trends in the busy legal profession.

Are websites tracking your every move and collecting your Internet browsing history? Today we want to discuss history sniffing: what is it, and can you do anything to stop it from happening to you?

Joining us in studio for today's discussion is Kristen Mathews. She's a partner at Proskauer Rose and is head of the firm's Privacy and Data Security group. Welcome back to the program, Kristen, it's nice to see you again.

K. Mathews: Oh, I'm happy to be here, Spencer.

S. Mazyck: Okay, so let's begin with the basics. What is history sniffing? Can you tell us how it works?

K. Mathews: Yes, I can. You ever notice that when you're browsing the Web, and you link from one page to another page and then go back, that the color of the link has changed, probably from blue to purple?

S. Mazyck: Yes.

K. Mathews: You have noticed that. Well, your browser is doing you a favor for your convenience by making it easy for you to tell whether you've been to a website or not. A couple of years ago, some folks realized that they could take advantage of that by figuring out whether a visitor to a website has ever been to other websites before.

S. Mazyck: Mmmm.

K. Mathews: And the way that they do it is they insert URLs onto a web page, but those URLs are covered or invisible so the visitor can't really see the URLs. However, they also plant some Java script code to read what color those URLs would be if they weren't invisible.

S. Mazyck: So the code is literally sniffing out your browsing history then.

K. Mathews: That's right.

S. Mazyck: So what's the difference between this history sniffing technique and Internet cookies, which I think are a part of most major websites?

K. Mathews: That's right. Uh, well, in history sniffing, no – nothing is planted or placed on the user's computer. But with cookies, a cookie is a file that is actually placed on the

user's computer. The file probably contains little more than a unique number just for you, so that when you come back to the same website later, that website will look on your computer to see if your – the cookie is there. If it's there, they'll know that you are the same person who was there before, and they might be able to link you with whatever they learned about it you the last time you – they were at your site. So it's another method of tracking people on the Web; it's just a different method.

S. Mazyck: But then cookies are designed to enhance the user experience on that website, correct?

K. Mathews: Mmm hmm.

S. Mazyck: Okay, and so what can websites do with your browsing history? Why is there so much concern surrounding history sniffing?

K. Mathews: Okay. Well, there's a number of different things you could do with it. One, you can see whether the visitors to your website have ever visited your competitor's website.

S. Mazyck: Okay.

K. Mathews: Two, you can see whether the visitors to your website have read specific other articles about you on other websites. In other words to find out what they already know about you.

S. Mazyck: Is it a way to target advertising, too?

K. Mathews: That's number three.

S. Mazyck: Okay.

(Laughter)

K. Mathews: They can share this information that they learn about you, *i.e.*, your browsing history, with advertising companies, and those companies can use it to create a profile about you and therefore enable them to target ads to your interests.

S. Mazyck: And I'd have to say that I think part of the concern with history sniffing is that, uh, it can be used for other things, uh, like discriminating even against someone who's sick from maybe even buying a car or renting –

K. Mathews: Mmm hmm.

S. Mazyck: – an apartment – uh, I don't know if that's part of the concern too, but, but –

K. Mathews: It's a theoretical possibility. I haven't heard it mentioned. One that I have heard mentioned, which is scaring a lot of people, is an identity thief could – if he can get you to his site – could plant some bank URLs, online banking URLs, on his site and detect whether you've been to that particular bank before, or which of those banks you've been to, and therefore find out what banks you probably have your money at.

S. Mazyck: Mmm hmm.

K. Mathews: How could they really use that? Potentially to make a phishing attack, uh, more likely to be successful. Do you know what a phishing attack is?

S. Mazyck: No, I don't.

K. Mathews: A phishing attack is when you send an e-mail to somebody – a thief does this – pretending to be, let's say, another company, like a bank, and the e-mail says, "Hey, we have a problem with your account. We need you to click here and log in to verify your account information," and the truth is that link is not really your bank, but rather an identity thief's.

S. Mazyck: Yes, I have – I have heard of that. With – with respect to history sniffing, do we have a sense of how many websites have engaged in history sniffing or are engaging in history sniffing?

K. Mathews: We do, because some folks at the UC San Diego, back in the fall, conducted a study. They surveyed 50,000 different websites, and they found that 46 of them were engaging in history sniffing, and then an additional 326 of them show evidence that they are probably also engaging in history phish – phishing – sniffing.

S. Mazyck: Well, are we all, um, vulnerable or at risk to having our browsing history sniffed, or are there certain Web browsers that are more susceptible than others to this practice?

K. Mathews: There are. Chrome and Safari, which are Google's and Apple's browsers, respectively, have both been patched so that this will not work. Firefox is going to be patched in their next release. The only one left that hasn't been patched is, um, Microsoft's Internet Explorer.

S. Mazyck: Okay, so let's say that you somehow discover that one of these websites is sniffing out your browsing history. Is there anything that you can do about it? Is there legal recourse to protect against history sniffing?

K. Mathews: Very good question. In fact, there are a few class actions that have already been filed against –

S. Mazyck: Yes.

K. Mathews: – some of the companies that are engaging in this.

S. Mazyck: And I want to talk about it, because I know that there were three class actions that were filed late last year, uh, against websites and companies allegedly conspiring with these websites –

K. Mathews: Mmm hmm.

S. Mazyck: – regarding history sniffing, and the first of them is against Midstream Media International. What does the complaint allege, and what are the plaintiffs seeking here?

K. Mathews: In that case, the plaintiffs are alleging that history sniffing violates a federal law called the Computer Fraud and Abuse Act as well as another federal law called the Electronic Communications Privacy Act as well as a few state laws. And they're basing these allegations on the simple facts, as I've described earlier, which are this website, which is called YouPorn.com – it's an adult website – have, um, included a bunch of competitor URLs on their page to determine whether their users have been to those other URLs.

S. Mazyck: Well – and it's interesting, because – and what are their plaintiffs seeking here, though?

K. Mathews: They're seeking, um, injunctive relief, meaning that they want them to stop doing it, as well as fin– monetary damages, attorneys' fees, and court costs.

S. Mazyck: Aren't the allegations in this case very similar to those contained in the second class action that was filed in late December, which is *Bose vs. Interclick*?

K. Mathews: They're very similar. There are some differences, though.

S. Mazyck: What are the differences?

K. Mathews: Well, in the *YouPorn* case, the YouPorn website is conducting this activity on its own website. Looking into it's own visitors' history. In the other cases, which are in California against Inter–

S. Mazyck: Interclick.

K. Mathews: – In– Interclick and some of its advertisers, um, those advertisers using Interclick's technology are actually history sniffing on third-party websites, not their own websites.

S. Mazyck: And – and that's pretty cool, actually.

(Laughter)

K. Mathews: That they could do that, right? How did they do that on someone else's website?

S. Mazyck: But (inaudible) that you're referring to, 'cause I know that the plaintiffs in the *Bose vs. Interclick* case two weeks later then filed a related class action lawsuit against McDonalds –

K. Mathews: Mmm hmm.

S. Mazyck: – CBS, I think it was Mazda Motor of America, Microsoft, and 50 John Does –

K. Mathews: (Laughs)

S. Mazyck: – and so was the complaint that these companies were conspiring with Interclick?

K. Mathews: Well, it wasn't a conspiracy claim. By the way, those cases have all now been consolidated –

S. Mazyck: Okay.

K. Mathews: – into one. Um, and the theory is that these advertisers are using Interclick's technology in order to find out, um, that – the browser history on third-party websites where these companies have posted ads.

S. Mazyck: Okay, and so tell me now, where are these class actions now in the litigation process?

K. Mathews: Well, the defendants – both Interclick and also these advertising defendants – have filed motions to dismiss. Um, arguing that even if all of the facts were true that have been alleged, those facts simply don't support a cause of action legally.

S. Mazyck: And so in your opinion, what's the biggest hurdle that these plaintiffs have to overcome in order to prevail in their claims?

K. Mathews: Mmm hmm. Well, under the Computer Fraud and Abuse Act, they would have to allege $5,000 worth of monetary damages. They've tried to da – do that in their ca– in their complaint. They've tried to say, "Listen, I could have sold this information about myself on the market." It's true that there is a lot of money being made in behavioral marketing. However, I don't know of a way that any individual could go and sell the fact – the information about where he's traveled on the Web. There's no market for it.

S. Mazyck: Right.

K. Mathews: So I think that's going to be a tough one for them to allege.

S. Mazyck: (Laughs) It sounds like it. So at the moment, though, the damages are undefined there?

K. Mathews: That's right.

S. Mazyck: Okay.

K. Mathews: And then the other federal claim, which is the Electronic Communications Privacy Act, is premised on there being – there having been an interception of a communication. Now, think about what I told you earlier. What's happening is there's a file that is stored on the user's computer that lists the websites that he's been to before. There's no communication. There's noth– there's no communication being intercepted. So I think it will be difficult for them to successfully allege that claim either, and, by the way, in the New York-based cases – which are the cases against Interclick and those advertisers – that ECPA claim has already been voluntarily withdrawn.

S. Mazyck: Oh, wow.

K. Mathews: Probably, in my view, for that reason.

S. Mazyck: And I think – didn't they also withdraw the wiretap –

K. Mathews: Yes.

S. Mazyck: – allegation?

K. Mathews: Yes. That's actually the same one. Wiretap and ECPA.

S. Mazyck: Okay. Okay.

K. Mathews: Mmm hmm.

S. Mazyck: Got it. Well, uh, how important is the outcome of these cases in protecting the his– the future of history sniffing litigation?

K. Mathews: Well, I can tell you that it seems like some of the companies that have been engaging in history sniffing have already backed off, maybe not because they're worried about the law, but because the media backlash –

S. Mazyck: Hmm.

K. Mathews: – has been very bad. As an example, I – it's reported that YouPorn backed off of this, and also several of the vendors of the technology that helps companies do this have discontinued those product lines.

S. Mazyck: But even if they've backed off, um, doesn't mean that it's not going to rear its head again.

K. Mathews: True. Mmm hmm.

S. Mazyck: So is there any – do we suspect that there might be federal intervention at some point, maybe regulating –

K. Mathews: Mmm hmm.

S. Mazyck: – history sniffing or other online activities – tracking activities?

K. Mathews: Mmm hmm. Well, there is a bill right now. Jackie Speier – it's called the Do Not, uh, Track Me Act. It's –

S. Mazyck: Oh, yeah –

K. Mathews: – federal.

S. Mazyck: – is – is it modeled after the Do Not Call registry, which I think most people are pretty happy for it, yeah.

K. Mathews: In concept, yeah. Uh huh.

S. Mazyck: Yeah.

K. Mathews: And it would enable – well, first of all, it would require companies to notify Web visitors of what they're doing. And secondly, it would require them to give their visitors a way to opt out of it. So that would be an example of, um, federal intervention on the legal side.

S. Mazyck: Well, and if under that legislation, if it should come to pass, then would there be legal consequences for companies that chose not to respect a user's right to opt out?

K. Mathews: Yeah, there would be.

S. Mazyck: Okay. And where is this legislation now?

K. Mathews: (Laughs)

S. Mazyck: This is kind of my final question. Are we going to see it, uh –

K. Mathews: Well –

S. Mazyck: – is it going to be signed into law tomorrow?

K. Mathews: No.

S. Mazyck: Or next week?

K. Mathews: (Laughing) I would have to say no. We don't really know if it's going to get passed. I can tell you that I've been tracking privacy – federal privacy legislation for a decade and a half, and every year there's a handful of privacy bills introduced, and every year passes and – and nothing gets passed. So will this happen? It's possible. Maybe this year's the year. Um, but I wouldn't put it at more than 50%.

S. Mazyck: Okay. 50% chance –

K. Mathews: (Laughs)

S. Mazyck: – of it passing. We're going to leave it there. But I have to say, if it does pass, it's certainly one way – a simple way that users can say "No, thanks" to being surfed –

K. Mathews: Mmm hmm.

S. Mazyck: – being tracked while surfing on the Web. So thank you very much –

K. Mathews: (Laughs)

S. Mazyck: – for sharing –

K. Mathews: You're welcome.

S. Mazyck: – your insight with us. We really appreciate you joining us.

K. Mathews: My pleasure.

S. Mazyck: When we come back, our spotlight on contributed content. We'll be back in a moment.

Announcer: Digital technology has transformed the way we live our lives. We can access any piece of information at any time from anywhere. We can share ideas with thousands of people instantly. Staying up to date with breaking news and events

is easier now than ever before. All this lets us keep pace with the world in real time. Yet, have any of these innovations been applied to the way we research and practice law? Starting today, the answer is yes.

Welcome to Bloomberg Law, the first and only real-time research system for the 21st Century legal practice, created by the leading provider of data and information services.

A single search feature with access to legal, news, and company databases provides you with powerful legal research results and a holistic view of your clients, filtered so you know the information you receive will be relevant every time. Customizable legal, financial, and news alerts keep you ahead of your clients and in tune with their world. An integrated workspace allows you to organize your results by client, by urgency, by topic – however you want it. And to share those results with people on your team.

Log in now to experience Bloomberg Law.

S. Mazyck: Now it's time for our spotlight on contributed content. This is a segment where we highlight an article that was featured in one of our Bloomberg Law Reports.

Today's article comes to us from Andrew Elbon of Bradley Arant Boult Cummings. The title of the article is, "New Era in HIPAA Privacy Enforcement? Recent Developments May Mean Greater Scrutiny Than Before."

Recently the Department of Health and Human Services imposed civil penalties for violations of the HIPAA privacy rule, which happened for the first time since this law was enacted. This article spotlights those actions and explains why they took place now and what they mean for other organizations required to follow HIPAA. You can find this article in this month's issue of our Bloomberg Law Report, Privacy and Information on the terminal at PILR Go or at bloomberglaw.com.

Articles are contributed to us for publication by practitioners, law professors, and other legal experts. To find out more about how you can contribute, please visit bloomberglaw.com.

A special thank you to Andrew Elbon for that contributed piece, and again, our thanks to Kristen Mathews of Proskauer Rose. Bye, everybody.