Social Networks & Privacy

Kristen Mathews on Bloomberglaw.com

S. Mazyck: Hello, everybody, on this Monday, November 8th, 2010. I'm Spencer Mazyck, and this is the Bloomberg Law podcast, a series of interviews focusing on trends in the busy legal profession.

Today we want to discuss social networks and information gathering: how does it all work, and what are the privacy concerns? Joining us in-studio for today's discussion is Kristen Mathews. She's a partner at Proskauer Rose, and as head of the firm's Privacy and Data Security Group. Welcome, Kristen, and thank you for joining us today.

K. Mathews: Well, thank you for having me. I'm very happy to be here.

S. Mazyck: Sure. Let's begin with: What are social networking sites, and what do they offer users?

K. Mathews: Okay. Well, the answer depends a lot on your definition of "social networking." The quintessential social networking site would be MySpace or Facebook, where a user, first of all, signs on to the site –

S. Mazyck: Mmm hmm.

K. Mathews: – and once he or she signs on, is able to connect with other users of the same social network.

S. Mazyck: Okay.

K. Mathews: Some of that connection manually – in other words, the user looks for somebody, maybe somebody from school or from a past life, and other connections are made through a more automated fashion, where the service actually recommends people that they think you may know or people that they think you may have commonalities with.

S. Mazyck: Well, something like a Match.com or eHarmony and Nerve – that would be more like what you're talking about?

K. Mathews: I would construe those as a subset of social networking. Match.com, eHarmony – they are social networks, but for a specific purpose, *i.e.*, finding a date or finding a friend.

S. Mazyck: Okay, I remember when sites like Friendster and MySpace were created, many people thought that this way of communicating with family and friends would be a fad, but is it true that social – isn't it true that social networking use is on the rise?

K. Mathews: It is. I wouldn't call it a fad any more.

S. Mazyck: (Laughs)

K. Mathews: The last I heard, 75% of teen and young adults were on a social networking page of some form, and 40% of adults.

S. Mazyck: Wow.

K. Mathews: And another statistic is that 25% of the time that people spend online is spent on social networking platforms, which is higher than any other online activity.

S. Mazyck: Wow. Well, so let's talk about the ways that social networks collect user information, and of course the most obvious wave is by users providing information directly to the sites.

K. Mathews: Yep.

S. Mazyck: What does user-provided information include?

K. Mathews: Well, it depends on which social network you're talking about, but essentially the user-provided data includes the registration information – usually an e-mail address, a user name, gender, date of birth – basic information about the individual is submitted when you create the account.

S. Mazyck: Well, and on some sites, might it also include transactional information if purchases are made on the site?

K. Mathews: Absolutely. Once you register, that social network is going to learn about you over time based on what you do on the site. So maybe you access a certain other user's page, or maybe you view a certain article, or maybe you buy something on either the social network itself or even on another web page.

S. Mazyck: Hmm.

K. Mathews: All of that activity becomes "user-submitted information," and the social networks do track that type of activity, and they use it.

S. Mazyck: Well, so what other ways do social networks collect user information?

K. Mathews: Well, we've talked about user-submitted data, but there's also data that is passively collected by a social network using things like cookies and web beacons, which you may have heard of.

S. Mazyck: Yes.

K. Mathews: What that means – maybe you've heard of clickstream data. What it means is that, from a technology perspective, the website – in this case, the social network – is tracking your passive usage information: information about what browser you use, what language the browser is configured to speak in, they can often find out a lot of information about you using your IP address. IP addresses could lend towards knowing what geographical location you're in.

S. Mazyck: Wow, so that's a lot of information that the social networking sites can gather, correct?

K. Mathews: Yes, even without the user having actively given it to them.

S. Mazyck: Might they also get information from third parties like applications and advertisers?

K. Mathews: Yes, they do.

S. Mazyck: Okay.

K. Mathews: First, they give data to applications in order for those applications to do what they're supposed to do. But after those applications have performed their function, they also send data back to the social networking site – data about what the user did with the application, for example.

S. Mazyck: Okay, and some privacy groups have said that social media is a threat –

K. Mathews: (Laughs)

S. Mazyck: – to personal privacy. Do you agree with that statement?

K. Mathews: You know, it's an interesting statement. In a way, it's true, and let me tell you what I mean by that.

S. Mazyck: Please.

K. Mathews: Over the course of the years, the existence of social networking has caused people's expectation of privacy to get lower. Five years ago, even a teenager probably wouldn't have expected for, let's say, Facebook to be doing some of the things they're doing, but since they've done it –

S. Mazyck: Hmm.

K. Mathews: – and years have gone by and they're still doing it, consumer expectations have changed. And what does that mean for the law? Well, the law follows expectations. Laws are designed to require that companies meet consumer expectations. So when, over time, social networks push the envelope – as they have – and continue to do so, consumers begin to expect

it, and the laws, therefore, conform to that. And that is what has happened, and that is why, in a way, what you said is true.

S. Mazyck: Well, so tell me this, though – the debates surrounding privacy in social networking – does it come down to who controls the disclosure of personal, private information?

K. Mathews: Disclosure is a big piece of privacy. For the most part – and again, this really is a moving target, because it depends on how consumer expectations change over time – but for the most part, consumers are not that appalled by Facebook's own use of what they learn about their users. The thing that makes them a little more suspect is Facebook's sharing of data with somebody else.

S. Mazyck: And I wanted to get to that. Speaking of disclosing personal, private information, Facebook has come under fierce criticism of late with the way that it handles user privacy, and the complaints are really about privacy breaches that were committed by its top-ranked applications. Can you tell us a little bit more about what happened there?

K. Mathews: Yeah. Well, first of all, the *Wall Street Journal* article that you're referring to – a lot of people, when they read it, they just couldn't understand what was being said. And that's because, in order to understand what happened in that case, you have to understand two elements of Internet technology, and most people don't understand these technologies. So let me tell you what they are.

S. Mazyck: At least not very well.

K. Mathews: Not very well. Thank you. One thing that you need to know is that – well, I'll put it to you this way: when you're browsing the Web, on any website, have you noticed that, as you link from one page to another on that website – maybe you searched for things on the website, maybe you view things on the website – have you noticed that the URL in the location bar of your browser becomes populated with code that may look like gibberish to you?

S. Mazyck: Mmm hmm.

K. Mathews: Digits and numbers and characters and plus signs and – have you – have you noticed that?

S. Mazyck: I've never noticed it, actually.

K. Mathews: Really?

S. Mazyck: No, I haven't.

K. Mathews: A lot of people don't notice.

S. Mazyck: Yeah.

K. Mathews: So as – the reason that happens is because as you browse the website and do various things on the site, the URL becomes to be populated with code that reflects what you've done on the site. And we call that "URL referrer information." So keep that in mind.

S. Mazyck: Okay.

K. Mathews: And let me tell you the second thing you need to know. When you browse the Web, the page to which you go, by definition, sees the URL from which you came. That is a necessary part of how the Internet works.

S. Mazyck: Okay.

K. Mathews: It's a technology necessity.

S. Mazyck: Mmm hmm.

K. Mathews: Okay? So combine those two things. One: the URL stores information about you, what you've done on a site. Two: the next page you go to, by definition, sees that URL. What you get, then, is a "disclosure" of information about what you did on a site to the next page you go to.

S. Mazyck: Okay, so I understand that, and how does it relate to the *Wall Street Journal* article?

K. Mathews: Thank you. In the *Wall Street Journal* Facebook situation, what happened was Facebook application vendors had to – and appropriately did – receive user ID numbers of Facebook users. They needed to have those numbers in order to perform the services that they perform. And in performing those services, they work with third parties. So keep track. We have three levels: we have Facebook, we have the application provider, and then we have these third –

S. Mazyck: Parties.

K. Mathews: – party companies. When the application provider works with these third-party companies, in some cases, they have to – to do this – to provide the service, provide the URLs.

S. Mazyck: Okay.

K. Mathews: So suddenly, this third level has that URL. That URL contains code that tells them where that person was on the Facebook page. And here's the rub: that URL on Facebook – and on MySpace, and frankly, on a lot of

sites – contains a code number that consists of the user ID number.

S. Mazyck: Okay. Well, and I understand that. And in some reports have said that the ten most popular Facebook applications like Farmville and Texas Hold 'Em poker – they were transmitting this information to the other outside companies, but tell me, what can somebody do with a Facebook ID number? What value does it have?

K. Mathews: Well, once you have the number, you can go back to Facebook, and pull up that Facebook user's profile or, similarly, from MySpace, okay? And so at that point you'll be able to see whatever is on that user's profile.

S. Mazyck: And I've heard the name Rapleaf –

K. Mathews: Yeah.

S. Mazyck: – connected with this. How are they involved here?

K. Mathews: Rapleaf –

S. Mazyck: And what is it exactly?

K. Mathews: Rapleaf is a company that harvested the URLs that they received, grabbed those numbers, and then went back to Facebook and gathered as much information as they could from these profiles, added it to their already pre-existing database of all Internet users –

S. Mazyck: Mmm hmm.

K. Mathews: – and essentially supplemented their knowledge that they already had about every Internet user, almost, added to that knowledge whatever they could glean from Facebook, and then sold the information to their customers. One example of customers to which they sold this information was political candidates, who would use it in order to target ads to – campaign ads.

S. Mazyck: Wow. Well, and Facebook said that this is against their policy, and it has addressed the controversy by saying, "We have proposed a technical solution to prevent this sort of transfer in the future. In addition, we are working with vendors to address this issue more broadly across the Web."

K. Mathews: Right.

S. Mazyck: The social networking site also said that they asked ad companies who retain this information to delete it –

K. Mathews: Mmm hmm.

S. Mazyck: – and then also any developer that received payment for transmitting this

information has been placed on a six-month moratorium.

K. Mathews: Mmm hmm.

S. Mazyck: But I want to move on and talk about Twitter, because it, too, has come under fire for some high-profile data breaches, and with that, could you tell us about a couple of breaches that occurred in 2009?

K. Mathews: Absolutely. So in the Twitter situation, hackers were able to hack into Twitter employees' e-mail accounts, okay, administrative accounts on Twitter. And once they got into those Twitter administrative accounts, they were able to then break into legitimate Twitter user accounts and, let's say, send out tweets –

S. Mazyck: Mmm hmm.

K. Mathews: – pretending that they were that user. The most well-known example is President –

S. Mazyck: President-elect Obama, right, I remember.

K. Mathews: Do you know what the tweet was?

S. Mazyck: I don't remember what the tweet was.

K. Mathews: It was, "If you fill out this online survey, I'll get you a $150 gasoline voucher."

S. Mazyck: Oh, wow. And this was when gas –

K. Mathews: Uh huh.

S. Mazyck: – and gas is still very high, but certainly gas was very high at the time, too.

K. Mathews: And, you know, the way that this happened is that Twitter's password rules that they had within their company for their employees weren't strong enough. So as an example, the passwords that were compromised were dictionary words, all lower case, no numbers, no @ characters. In addition, they didn't have it set up so that after you put in the wrong password, let's say 10 times, it would lock you out. And the way that some of these passwords were compromised is by password software that just puts in every password until it gets one. So if the site had been set up to block people out after X number of wrong passwords, that would have rectified the situation.

S. Mazyck: No, go ahead. Continue.

K. Mathews: The other thing that's very interesting about what happened with Twitter is

that one of the methods that the hackers used to compromise the Twitter employees' admin accounts was by first compromising that employee's personal e-mail account.

S. Mazyck: Hmm.

K. Mathews: Probably web-based e-mail accounts.

S. Mazyck: Right.

K. Mathews: You ever notice that when you have a web-based e-mail account, when you create it, they want you to answer these security questions?

S. Mazyck: Yes. Security safety questions.

K. Mathews: Like what street did you grow up on or what was your high school mascot.

S. Mazyck: Or your mom's maiden name.

K. Mathews: Yeah. Think about the kind of information that you can get on somebody's Facebook page.

S. Mazyck: A lot of information, I imagine.

K. Mathews: And a lot of information that is in those typical security questions.

S. Mazyck: Well, these incidents led to a probe by the Federal Trade Commission of Twitter's business practices and the way that it handles users' information.

K. Mathews: Mmm hmm.

S. Mazyck: And it ultimately resulted in a consent order between the parties. The consent order said what?

K. Mathews: Well, it said that they had to change their practices.

S. Mazyck: Okay.

K. Mathews: And they have to be audited – I don't know how frequently, but oftentimes it's every two years. And in the future, if they ever fail to have "reasonable data security measures" again and they suffer a breach, they could suffer monetary damages.

S. Mazyck: And the order also barred Twitter for 20 years from misleading consumers about the extent to which it protects their security, privacy and confidentiality of users' personal information, but I find that interesting because – well, what happens after 20 years? Are they then able to go back and start misleading consumers? (Laughs)

K. Mathews: The only difference is the monetary damages that are available during the 20 years versus after the 20 years.

S. Mazyck: Okay.

K. Mathews: They're never allowed to mislead.

S. Mazyck: (Laughs)

K. Mathews: And that's why they suffered the settlement in the first place.

S. Mazyck: Right.

K. Mathews: A lot of websites, if you read their privacy policies, there's a security section that says, "We use reasonable methods to protect the security of the information you provide." The FTC uses those promises and those privacy policies, and they hold companies to those promises. And that's what they did to Twitter.

S. Mazyck: And I want to move on and talk about our last data breach today, and that is – involves Google.

K. Mathews: Mmm hmm.

S. Mazyck: It happened earlier this year with the launch of Google Buzz.

K. Mathews: Mmm hmm.

S. Mazyck: What is Google Buzz, and what are the privacy concerns surrounding its launch?

K. Mathews: Well, Google launched its social networking platform. It competes with Facebook. And when they launched it, they knew that they already had a lot of Gmail users – users of their Web-based e-mail service. And they wanted to take advantage of that subscriber base that they already had, and so they defaulted them into the Buzz service.

S. Mazyck: So every Gmail user then became a participant in the Google Buzz.

K. Mathews: In a way, yes. What happened was, they created template, if you will, or starter Buzz accounts for these Gmail users and pre-populated the accounts with information that they knew about the users because of the Gmail.

S. Mazyck: Hmm.

K. Mathews: So, for example, they knew the e-mail addresses that you most frequently send and receive e-mails to and from. And they pre-populated your follow list with those e-mail addresses.

S. Mazyck: Well, and I also know that whenever you – if you used a mobile device or anything containing a GPS to access Buzz, it would determine your location, map your coordinates, and then publish that to everybody in your address book, which –

K. Mathews: (Laughs)

S. Mazyck: – I can imagine why folks might want to opt out of that. (Laughs)

K. Mathews: Yeah. You know, location information is a really hot button, especially now. In fact, one of the fastest-growing Internet or online activities is mobile activities. And when you participate in a mobile app, that application service provider is going to know, or potentially know, where you are at that particular time. Now, the laws, when it comes to location information, actually are a little bit more – a lot more protective than the laws that apply to, you know, e-mail address and interests.

S. Mazyck: And why is that?

K. Mathews: Well, because it's more sensitive. The physical – the place where you're at at a particular time could be used against you, let's say, by, you know, an ex-spouse.

S. Mazyck: Right, somebody who's stalking you –

K. Mathews: Mmm hmm.

S. Mazyck: – or somebody who wants to find you for –

K. Mathews: Yeah.

S. Mazyck: – for some reason or another.

K. Mathews: So even the laws in this country, which are pretty permissive when it comes to privacy, treat location-based privacy a little bit more protective than they do other.

S. Mazyck: And with respect to – getting back to Google Buzz –

K. Mathews: Yeah.

S. Mazyck: – with respect to that, did it result in a class action by the Gmail users?

K. Mathews: It did. And that class action was settled recently. And the result was that Google paid the lawyers a lot of money –

S. Mazyck: (Laughs)

K. Mathews: – and they also paid a – in my view, a small amount of money to the named plaintiffs, okay. And then they put a lot of money – I mean, everything's relative, maybe to them it's not a lot of money – but the rest of the $8.5 million is being put in a fund that's going to be used to study and educate on privacy issues.

S. Mazyck: Hmm.

K. Mathews: Now the interesting thing that didn't happen as a result of the settlement is that Google didn't agree to turn this Buzz into an opt-in service. They're continuing their opt-out regime.

S. Mazyck: Well, does that mean, then, the Gmail users that they signed up for it, are they still going to be signed up until they decide to opt out of it?

K. Mathews: That's right. What they did do is, they are sending a lot of messaging out to the users, telling them, "By the way, go into your privacy settings, because if you don't, the default position is that you're on – you're on Buzz, and this is what's happening." So they're sending messaging out trying to get everyone to go on and fix it.

S. Mazyck: Okay, and Epic also filed –

K. Mathews: Yes.

S. Mazyck: – a complaint with the FTC.

K. Mathews: Mmm hmm.

S. Mazyck: Did anything come of the complaint?

K. Mathews: Not yet. The last I heard, the FTC wouldn't admit – you know, they can't – they can't tell us if they're investigating a company –

S. Mazyck: Right.

K. Mathews: – because investigations are non-public. So the last I heard, they said, "We can't admit or deny that we're doing it." I have no knowledge at all, but I feel that they probably are investigating it.

S. Mazyck: Okay.

K. Mathews: Because it just seems to me that they would.

S. Mazyck: Well, and there are a lot of consumer groups – just changing subject just a bit – but there are consumer groups and privacy groups who are calling for restrictions and regulations on the way that social media handles users' privacy.

K. Mathews: Mmm hmm.

S. Mazyck: So are we going to see new Federal regulation in this area?

K. Mathews: Well, let me preface my answer by saying that for years, many years, there have been bills introduced, there have been Congressmen talking about it, there have been consumer protection groups talking about it, and the "it" is legislation, Federal legislation. And yet, for years, it has not happened.

S. Mazyck: With respect to social media? And privacy?

K. Mathews: Well, privacy in general.

S. Mazyck: Okay.

K. Mathews: Privacy in general, but it would include social media. Particularly it would include behavioral marketing.

S. Mazyck: So now that you've said that, though –

(Laughter)

S. Mazyck: – are we – is there any legislation?

K. Mathews: So one would look at the past 10 years' history and say "They haven't done it yet; they're not going to do it now." That said, though, the issue is getting more and more intense as the years go by, and the social networks – not to mention every other online company – are pushing that envelope more and more every year. So it wouldn't surprise me if we got legislation, but let me tell you this: if we do get legislation, I don't think that it's going to require much different than what the industry has already begun to do voluntarily. In other words, they have adopted this notice and choice regime, meaning, "As long as we tell everybody what we're doing, and we gave them the right to opt out, we should be good to go."

S. Mazyck: So then, as a general rule, then, are companies saying, "Well, it's okay to collect individuals' information unless that individual opts out of the collection"?

K. Mathews: That's what the industry's doing. That's what they've been doing for a long time.

S. Mazyck: But so when would it be okay for – well, I guess, what information would people want to give their permission or consent to prior to collecting?

K. Mathews: Okay. That's where we get to what we call "sensitive data." Precise location information is an example of sensitive data. For that, I think both the industry and the law, if we ever see it, would provide for an opt-in

regime for sensitive data. Another example of sensitive data would be sexual orientation, religion, health information, Social Security number. For that type of data, I would expect an opt-in regime.

S. Mazyck: Do you think that any kind of regulation in this vein might stifle innovation, though?

K. Mathews: No, because I don't think that the legislation that may be passed would be – would require much different from what the industry's already doing. In other words, I believe the industry is strong enough, the lobbyists are strong enough, to influence the legislation such that it's really not going to hurt what they're doing too much.

Now, I want to say one more thing: there's two proposed bills out there now. And both of them have this opt-in requirement that requires opt-in for use of sensitive information, which we've discussed, but they also require opt-in for "sharing" of information. And a lot of people have misunderstood those two pieces of legislation because the opt-in provisions in those bills have exceptions, and those exceptions are broad enough to essentially enable the industry to continue what they're doing.

S. Mazyck: And the bills that you're referring to, I know that there's one by Bobby Rush which is called the Best Practices Act.

K. Mathews: Yeah.

S. Mazyck: And then there's also one by Rick Boucher and Cliff Stearns –

K. Mathews: Yep.

S. Mazyck: – I think it's untitled at the moment.

K. Mathews: It's not titled, and it's not even introduced. It's a draft bill that they floated around last – maybe around May – around May of last year, and they've received comments informally, not as part of the Congressional process, but –

S. Mazyck: No, and they both applied to online and offline information.

K. Mathews: Online and offline. They define IP addresses as personal information. Boucher wasn't re-elected last Tuesday.

S. Mazyck: Yes. (Laughs)

K. Mathews: So –

S. Mazyck: I saw that.

K. Mathews: – it's interesting to think about what impact that will have on his proposed legislation, although it was co-introduced with Stearns. Stearns is still there. And also there's support within the Republican party for – just like there has been for years, like I said –

S. Mazyck: Mmm hmm.

K. Mathews: – for privacy legislation. So I don't know how much impact that will really have.

S. Mazyck: Okay, well, in our remaining moments, I'm going to ask you to do something for me. If you could imagine that you're looking at a crystal ball, could you tell us what the future holds for this area of the law?

K. Mathews: I can, because I've been watching it for – you know, my whole career, so I have a mind for what I think will happen. First of all, I do think that the industry – in particular, the heavyweight companies: Facebook, Google – they're going to continue to push that envelope as much as they can, because they know that the effect of that is to change consumers' expectation of privacy, and if they achieve that, it's going to mold the laws.

S. Mazyck: Right, which is what you said earlier.

K. Mathews: Exactly.

S. Mazyck: It ties into that.

K. Mathews: And notice how Facebook – they keep – you know, launching these new programs.

S. Mazyck: Pushing the envelope.

K. Mathews: Pushing the envelope. Pushing the envelope. They change their privacy policy every time they do that. According to the FTC, you can't make what we call a material adverse retroactive change to a privacy without permission, without an opt-in from everybody. They haven't been getting an opt-in from everybody. They're pushing that envelope, and they're taking the position that the changes they're making are not material. Or not adverse.

S. Mazyck: Right.

(Laughter)

K. Mathews: And I don't know if they'll be successful. They have been – they've been doing it successfully for several years. But as we've said, the FTC – they might be looking at both Google and Facebook right now, and we don't know 'cause it's not public.

S. Mazyck: All right, well, we're going to have to leave it there. We'll stay tuned to see whether or not your predictions come true. But thank you very much for sharing your insight with us today.

K. Mathews: My pleasure.

S. Mazyck: We appreciate it.

K. Mathews: Thanks for having me.

S. Mazyck: Of course.

When we come back, our spotlight on contributing content. Back in a moment.