Roundtable Series

February 2016

Privacy

Daily Journal • callawyer.com

Roundtable Series

Privacy

Long a dynamic practice area, the field of privacy law may be hotter than ever. The industry grabbed headlines last year as major breaches hit a slew of high-profile targets, from the IRS to the notorious adultery website Ashley Madison. In jurisdictions across the country, statutes and judicial decisions impacting data privacy and security are mounting, putting conflicting pressures on businesses and their attorneys. Meanwhile, practitioners are advising clients on litigation over data privacy and security breaches, evolving best practices, regulatory developments, and the increasingly robust insurance market.

California Lawyer moderated a conversation on these and related issues among Ian Ballon of Greenberg Traurig, Michael Hornak of Rutan Tucker, Rosemarie Ring of Munger Tolles Olson, Erik Syverson of Raines Feldman, and Dave Watts of NetFusion. The roundtable was reported by Laurie Schmidt of Barkley Court Reporters.[1]

Participants

IAN BALLON
Greenberg Traurig

MICHAEL HORNAK
Rutan & Tucker

ROSEMARIE RING
Munger, Tolles & Olson LLP

ERIK SYVERSON
Raines Feldman, LLP

DAVE WATTS
NetFusion

Moderated by
CALLAWYER.COM

DISCUSSION

MODERATOR: What privacy trends do you think will emerge in 2016?

ERIK SYVERSON: It's an election year, so I think one trend that we might see emerge, given some of the saber-rattling that has already happened with some of the candidates, is this tension between personal liberty and national security as it relates to terrorism. Politicians at every level, from your local city councilmen, on up to the Presidency, obviously are invested in this, because everyone's lives are affected by data breaches and privacy issues now.

I'm also predicting a rise in negligence-based class actions, especially in California and in Illinois in the Seventh Circuit. It'll be interesting to see how the duty and causation elements evolve, and also what sort of facts support breaches of duty to protect consumer information.

We'll also see increased SEC enforcement. In 2015 we saw that begin with rogue traders and pilfered insider information. In 2016, the law firms that do big M&A deals will really be targeted, because there's an incredible amount of money that can be made from trading that information. The SEC will have to step up their game in prosecuting those cases.

I anticipate more small enterprise—$50 million to $200 million privately-owned, often family businesses—being increasingly targeted because it's low-hanging fruit for the bad guys. Big consumer-based companies have really stepped up their cybersecurity game, so this is one way for bad guys to make a quick, easy buck.

1 The views expressed are only those of the speakers and not those of their firms or clients.

IAN BALLON defends data privacy, security breach, and TCPA class action suits. He authored the four-volume legal treatise, *E-Commerce and Internet Law: Treatise with Forms 2d edition* (West), and books on security breach notification laws and the CAN-SPAM Act. A Chambers-recognized lawyer, Mr. Ballon was recognized by *The Daily Journal* both as one of the Top 75 IP litigators in California (2009 through 2015) and as one of the Top 100 lawyers in California.

Ballon@gtlaw.com

gtlaw.com

Finally, board level involvement at companies is going to have to ramp up. If you're a corporation, you need to think about appointing someone to your board who has really delved into these issues, and can lead a committee and make sure that the company's privacy hygiene is up to snuff.

DAVE WATTS: I agree, the small- and medium-sized businesses are going to be at an increased risk of becoming targets. According to Verizon's 2015 Data Breach Investigations Report, organizations with 11-100 employees are attacked 15 times more often than those with less than 11 and more than 100 employees. So I do agree that the big boys have upped their game. The small businesses don't necessarily have the same resources or the sophistication or even the knowledge of their own risk.

I also think the frequency and severity of breaches is going to dramatically increase due to two factors: first, there will be the increasing number of attack vectors. So you've got a proliferation of devices per person, and proliferation of locations from which they access data. All of that has to be secured differently. It's like you're protecting a home—except it has seven front doors and the house moves on a daily basis. That proliferation is going to make things much more difficult.

Second, I think the frequency and severity of breaches will increase due to the reduced bars for entry to professional cybercrime. The market has been divided up into wholesalers and retailers of tools being used to perpetrate cybercrime, and it is very inexpensive. You can even buy an exploit kit on the black market for as little as $200 and be in the cybercrime business. That's bad news, and we need to prepare for it.

IAN BALLON: A year from now, the landscape is going to look very different. The question is, in what respect.

In the privacy area, the U.S. Supreme Court's decision later this year in *Spokeo v. Robins* is going to be very important, because the Court may decide that Article III standing is an independent constitutional requirement, which would eliminate a whole range of privacy cases.

In the security breach field, there is almost a circuit-split in the way courts are looking at standing. At some point that will be resolved, but I don't think it will be within the next year. In the meantime, this split means that where you sue or are sued can be outcome determinative.

In TCPA cases, we will continue to see fallout from the FCC's 2015 regulations. The regulations are perceived to be very consumer-friendly, but they also potentially make it more difficult for plaintiffs to certify class actions in certain cases. I defeated a motion for class certification in one putative class action, in part, because the new regulations required individualized inquiries of whether consent had been given and, if given, revoked through any reasonable means (within the meaning of the regulations). In the coming year, we may find other courts concluding that the new regulations make certification of class action suits more difficult for plaintiffs.

The presidential election also could influence the direction of regulation and, by extension, class action litigation. Over the past eight years we've seen a more aggressive regulatory environment take hold in Washington D.C. than we saw in the Clinton or Bush administrations. Over the next four years, will we continue to see privacy, TCPA, and security enforcement pushed very aggressively through enforcement actions and punitive measures or will there be some pullback and more of a focus on more

MICHAEL HORNAK is a senior partner at Rutan & Tucker and heads the firm's Cybersecurity, Privacy, and Corporate Governance practice. His expertise extends to intellectual property disputes, shareholder and partner governance, the defense of consumer and shareholder class actions, and commercial litigation. He has been repeatedly recognized as one of the Best Lawyers in America (Woodward/White). He is a former managing partner of Rutan & Tucker, and heads the firm's Technology Committee.

mhornak@rutan.com

rutan.com

business-friendly regulations?

ROSEMARIE RING: Practically speaking, I think companies that deal with credit card data will get more clarity on how to process and protect that data to avoid privacy issues and to ensure strong defenses if there is a breach and resulting litigation. There were court decisions and an FTC settlement that provide very helpful guidance. That said, they also left open big questions about what constitutes injury under the FTC Act.

I think another area that will get a lot of attention is how companies deal with third parties who have access to their data. We've seen lawsuits this year by companies against security firms and other vendors that consult on IT and system-related issues.

Thinking about what information can and cannot be shared with third parties raises another issue: what is personal information? We've seen this play out in the context of Video Privacy Protection Act cases this year, which turned on whether anonymous identifiers can constitute "personally identifiable information" under the VPPA. Companies who share customer data with a third party are going to have to keep much tighter controls on them.

MICHAEL HORNAK: In the next year, I see a growing effort by both the public and private sectors to come to the plate and spend more on cybersecurity. Municipalities haven't had to worry too much because most of the data they have is not online. But with the recent passage of AB 169 (Gov. Code, § 62530.10) and SB 272 (Gov. Code, § 6270.5 in California, there are two new requirements in place: By July 1, municipalities and agencies must catalog all the public data they are holding; and two, if that data is going to be made available on the Internet, it must be open source.

So municipalities and cities must start asking: What are we going to make available online? What are the privacy concerns? How do we remove Social Security numbers and personal identifying information? The public sector will start having to deal with things the private sector has dealt with for a long time.

In the private sector, I see large companies that do business in Europe reexamining their policies. There's a tentative agreement between the European community and the U.S. Department of Commerce that will lead to stricter data standards. I suspect they're going to require some recertification to meet the requirements of the new safe harbor.

And lastly, to elaborate on Erik's point about board-level involvement, Senator Reed introduced some really interesting legislation in December, which would require all public boards to have a cybersecurity expert, and if they can't comply within a year, explain why they haven't been able to comply. So it's going to be a very interesting discussion during the next year.

MODERATOR: How are companies differentiating between legal requirements and best practices? What are some of the best practices you're seeing now?

BALLON: It is a challenge, because many of the laws governing privacy and security look to reasonableness standards for good reason – because technologies constantly evolve and what is reasonable today may not be tomorrow. If statutes or regulations enshrined current standards of encryption or other protective measures, they would rapidly become obsolete. At the same time, the flexibility of a reasonableness standard means that companies are forced to confront a moving target.

As a consequence, and because of

ROSEMARIE RING is a litigation partner with Munger, Tolles & Olson LLP whose practice focuses on complex commercial litigation with an emphasis on privacy and consumer class actions and intellectual property disputes. She has represented technology companies in litigation and government investigations involving a wide variety of products and services, including online social networking, streaming digital media, mobile devices, software, cloud platforms, computers, gaming consoles and various telecommunications services.

Rose.Ring@mto.com

mto.com

the threat of litigation and a lack of safe harbors, businesses feel pressure to do more than what may be reasonable. This, in turn, changes the definition of what is reasonable. If a large corporation does X, is it reasonable for a smaller company not to employ the same measures? What is reasonable in the abstract depends on the type of threat and the size of the company.

WATTS: The legal requirements are often intentionally vague and unspecific because they are going to change as technology changes. But that becomes very difficult for small or medium-size businesses. As a result, many businesses are starting to work with professional advisors—attorneys, CIOs, CSOs—to implement best practices based on ISO standards, the SANS Institute, among other resources. Those are industry standards, and they're free to look up. Whether or not small businesses know to look them up is a different matter. But they are actionable, specific, and measurable tools.

There is a need for more resources tailored to smaller businesses because they can't always afford professional advisement, and they seek things that they can look up themselves. But for small businesses, the first step is knowing that their business is at risk and where they're at risk, and then hopefully taking action after that.

RING: I've seen a movement among my clients to make data privacy and security part of their corporate culture. It may not be possible to prevent a breach. But if you are thinking about privacy when developing a new product or service—e.g., how you collect, use, and store data—security follows. This kind of awareness has to be built into the culture, it can't just be a legal issue.

WATTS: It's important to remember the human perspective and operational controls. I've seen companies "gamify" their strategies to encourage employees to be alert and look for things that are possible breach risks. For example, I've seen companies give a Starbucks gift card at the end of the month to the employee who avoids clicking on the most phishing attacks. By making it a game, you actually make people conscious of the issue. Many phishing-related problems happen because people are just unaware of the issue.

MODERATOR: How are company best practices evolving in relation to vendors?

RING: Disclosing or allowing access to data by third parties can create huge risks. But it also has to be done. So companies have to understand and monitor what these third parties are doing with the data, impose limits on it, and provide for indemnification. I've seen that more and more frequently.

SYVERSON: I'm amazed and shocked at what I see in my clients' vendor contracts with payment processors on what needs to be done in the event of a breach. I often see zero language about my client's responsibilities, the vendor's responsibilities, or details on the assessment process. That sloppiness on the part of payment processors has come back to bite them. In *Schnuck Markets, Inc. v. First Data Services Corp. et al.*, case number 4:13-cv-02226 in the U.S. District Court for the Eastern District of Missouri, the Court disallowed certain assessments levied by the payment processor because those assessments were not laid out in the retailer contract.

I also see this sloppiness in contracts with outside hosting services. I've had clients who don't even know where their data is. It might be halfway across the globe, and you don't even know if

you have a right to access it so you can provide it to your forensic experts, or more importantly, the FBI or the California Attorney General.

HORNAK: To put it in the perspective of the small or medium-sized company, when you sit down and look at a typical commercial contract, you're going to see exclusions of consequential damage liability. In the past, people thought nothing of it—this is a commercial contract. But this is an example where you need to negotiate a provision to ensure that that your vendor is complying with requirements, has insurance, and is going to be responsible, because you are going to be responsible, ultimately, for the breach that happens at the company.

WATTS: Segmentation of your networks is a recommended best practice. There's usually no reason to have networks with a flat hierarchy. You should be able to segment things away so that a vendor can't present an unnecessary risk. They shouldn't even be on the same subnet as your production data.

RING: Segmentation is also becoming a focus in litigation. It figures prominently in both the Wyndham FTC settlement and the Adobe data breach case. It is as near as can be to an industry standard—companies that ignore segmentation of their systems are doing so at their peril.

HORNAK: I agree. The need for segmentation is so important, because it's a world where we can never protect against all breaches, so we have to reduce the effects of the breach. One of the reasons we have this issue with segmentation is that many companies, if they grow quickly, have very flat networks. So proper segmentation would require significantly restructuring their networks.

WATTS: Also, we keep talking about it from the perspective of the client versus the third-party vendor. Third-party vendors should be asking the client, "What are you going to do to prevent me from having any possible access to anything I'm not supposed to see?" It should be a two-way dialogue to show some responsibility on the vendor's part.

MODERATOR: How are companies handling security breach notification requirements? Do we need a federal standard?

BALLON: A federal law today would not be helpful to businesses unless it included an express safe harbor that limited the risk of litigation. The problem in this area is that there are 47 state security breach notification statutes, as well as statutes in effect in Washington D.C., Puerto Rico, and Guam. There are multiple different and in some respects incompatible requirements that companies must follow when a security breach impacts residents of all states and territories. But as lawyers we have been dealing with this regulatory landscape for several years now, so we know how to respond to breaches and comply with the requirements. Adding an additional layer of regulation at this point would not be helpful unless it created a safe harbor to insulate a company from litigation.

SYVERSON: Well, I'll be a little contrary. I actually think it would be helpful to get some sort of federal law that preempts the conflicts in state law, even if there is not a safe harbor. Yes, we know how to deal with the conflicts, but I'm just kind of sick of dealing with them and so are my clients because it costs money.

Segmentation is also becoming a focus in litigation. It figures prominently in both the Wyndham FTC settlement and the Adobe data breach case. It is as near as can be to an industry standard—companies that ignore segmentation of their systems are doing so at their peril.

– ROSEMARIE RING

ERIK SYVERSON is a partner with Raines Feldman, LLP in Beverly Hills. He leads the firm's cyber liability practice. Erik and his team frequently represent small to mid-market companies in data breach and privacy suits, trademark, copyright and patent litigation, and Internet based defamation litigation. Additionally, Erik and an international consortium of lawyers represent a group of terror victims with over $250 million in legal judgments against Iran, Syria and North Korea.

esyverson@raineslaw.com

raineslaw.com

HORNAK: It is easy for a big company to deal with the 47 different notice requirements and the conflicts between them. But we need to be there for the smaller-size companies who have difficulty dealing with this—for example, a medical practice group that has to deal with all the various laws that apply to protecting patient data.

WATTS: Do you think small- and medium-sized businesses are actually notifying people in the event of breaches? Do you think they are also unaware that they even have to notify people, or under what circumstances they have to do it?

HORNAK: Some are unaware, but I have seen medical offices that were aware of the requirements. Those in regulated industries, highly regulated under HIPAA, and the financial institutions are much more sensitive to the requirements.

SYVERSON: I've noticed some reluctance by businesses to reach out and cooperate in a timely manner—they sense a blame-the-victim environment. They fear hefty penalties by regulators and class actions. And if they disclose a breach, they are also afraid that their customer base will also evaporate. So they're in a tough spot.

RING: I don't disagree, but you have to get over that. If the fear is, "We're going to get in trouble because we haven't been paying attention to cybersecurity," then it will only be worse when it comes out later—and it usually does.

BALLON: I agree. It's the law, and frankly, a good practice to notify consumers of security breaches that could materially affect them. Even when a breach does not legally require notification under the technical requirements of a given state, it is sometimes in the interest of a company to provide notice in the interest of good customer relations. Also, if it comes to light that information was compromised and no notice was provided, a company could be sued for negligence or similar claims. Most class action suits arising from security breaches are premised on common law theories of recovery. Failing to provide notice—or failing to provide adequate or timely notice—increasingly is alleged in security breach cases.

WATTS: One of the things I would recommend to a business of any size is to have good logging of all systems. Because in the event of a suspected breach, you can get a professional to evaluate those logs and possibly determine whether or not you actually had a breach, and if so, the extent of the breach, and whether or not you need to notify someone. Without those logs, you don't really have much of a technical leg to stand on.

MODERATOR: What are some of the litigation trends you're noticing from last year that you think will carry on in 2016?

RING: Standing is a major issue. For years now, we've gotten rid of data breach cases by arguing that the "risk" of future harm, such as identity theft, was not sufficient injury to establish Article III standing. But that's been changing.

In 2013, a U.S. Supreme Court case, *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138 (2013), examined to what extent future harm can be concrete enough to establish Article III standing. The Court held that the harm must be "certainly impending." Many courts in data breach cases interpreted it as a higher standard—that you need evidence of actual identity theft or fraudulent credit

GT GreenbergTraurig

1900 ATTORNEYS | 38 LOCATIONS WORLDWIDE*

On the Cutting Edge of Global Privacy and Cybersecurity, Including the Defense of Data Privacy, Security Breach and TCPA Class Action Suits

We develop innovative strategies to counsel and defend industry-leading clients facing data privacy, security, and information management concerns.

This issue's Privacy Roundtable includes Ian Ballon, co-chair of Greenberg Traurig's Global Intellectual Property & Technology Practice Group and the author of the leading Internet law treatise, *E-Commerce & Internet Law 2d edition* (West, www.IanBallon.net). Ian defends data privacy, security breach and TCPA class action suits. He is listed in Chambers & Partners in the area of data privacy and in the *Best Lawyers in America* as the 2016 Lawyer of the Year in Information Technology Law. He also holds the CIPP/US certification from the IAPP.

IAN BALLON | ballon@gtlaw.com | 650.289.7881 | 310.586.6575 | Silicon Valley & Los Angeles

GREENBERG TRAURIG | CALIFORNIA

LOS ANGELES | ORANGE COUNTY | SACRAMENTO | SAN FRANCISCO | SILICON VALLEY

GREENBERG TRAURIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM

DAVE WATTS is president of NetFusion. Watts and his team design, implement and manage stable, scalable and secure IT networks for professional services firms and small-to-medium sized businesses throughout California. Recognized by the *Los Angeles Business Journal* as a finalist for CIO of the year for three consecutive years, Dave uses a proprietary approach to network architecture, designed to bolster an organization's productivity and network accessibility while increasing data privacy and security.

dwatts@netfusion.com

netfusion.com

card charges to demonstrate "certainly impending" harm.

But in 2014, in *In re Adobe Sys., Privacy Litig.*, No. 13-CV-05226-LHK (N.D. Cal. 2014), Judge Lucy Koh found *Clapper*'s "certainly impending" standard was met without proof of actual identity theft or fraudulent credit card charges. She took an intuitive approach: why else would hackers target Adobe, steal credit card information, and use Adobe's own systems to de-encrypt the credit card information, if not to commit identity theft or make fraudulent credit card charges?

Last year, the Seventh Circuit was the first court to follow that reasoning at the federal appellate level in a case called *Remijas v. Neiman Marcus Group*, 794 F. 3d 688 (7th Cir. 2015). The *Remijas* court focused on a "substantial risk" standard, but also found it was reasonable to assume that a targeted attack on Neiman Marcus's systems in which credit card information was stolen created the type of "certainly impending" harm required under Article III.

But these decisions also raise questions. Does encryption matter? What about reimbursement? In *Remijas*, the court said that even if you're reimbursed following a fraudulent charge, there is still cognizable harm because you have to get the charge reversed, get a new card, and so forth. We'll see what other courts do, but for companies who store credit card information the takeaway is the trend toward finding injury based on the risk of future harm—even without proof of actual identity theft or fraudulent credit card charges.

Finally, it will also be interesting to see where the U.S. Supreme Court comes out on *Spokeo*. Plaintiffs in privacy cases challenging how data is used generally bring statutory claims. In *Spokeo*, the Ninth Circuit held that alleging a violation of a statutory right is sufficient injury to establish Article III standing. An avalanche of privacy cases based on so-called "statutory standing" followed. We don't have a decision yet. But if the Supreme Court affirms the Ninth Circuit, we're going to see that continue.

BALLON: I agree. If the Supreme Court finds in *Spokeo* that Article III requires an independent basis for standing, it will have a greater impact on data privacy cases than on security breach suits because so many data privacy cases are brought under federal statutes. Security breach cases more typically are based on alleged breaches of common law duties under theories such as breach of contract, breach of implied contract, breach of fiduciary duty, and negligence.

But I have a different take on the significance of *Remijas*. It is true that the Seventh Circuit followed Judge Koh's decision in *Adobe*. If you look at the circuit split that existed before *Clapper*, the Seventh Circuit had one of the most liberal standards for standing (e.g., *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007)), as did the Ninth Circuit (e.g., *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010)). It is perhaps not surprising that courts in these two circuits have construed *Clapper* in a way that is consistent with earlier, more liberal case law. In fact, Judge Koh made clear in *Adobe* that although the U.S. Supreme Court used different terminology in *Clapper,* she construed *Clapper* as essentially consistent with *Krottner*. But I think *Clapper* actually *did* set a higher standard for establishing standing than what previously had been required. Numerous district courts from around the country have construed *Clapper* this way and it is more difficult today than it was before *Clapper* for a plaintiff to establish standing in a security breach case

where the plaintiffs' information has been compromised but the plaintiff has not been the victim of identity theft.

While it may be that because *Remijas* was the first circuit-level case post-*Clapper* to look at standing in a security breach case other circuits will follow *Remijas*, I believe that the better view is that *Remijas* applied *Clapper* too narrowly in a way that is consistent with pre-*Clapper* Seventh Circuit law and that other circuits may agree that post-*Clapper*, more is required to establish standing. *Remijas* does not signal a new trend as much as a continuation of circuit splits that existed prior to *Clapper.*

SYVERSON: I find *Remijas* the most interesting case of 2015. If you're a plaintiff's class-action attorney, this is the greatest case in the world. This is results-driven jurisprudence. Standing is so easy to obtain here that it's effectively telling companies that they must invest in impossibly high-level prevention.

For a number of years it's been relatively easy wins for the defense side by getting cases tossed out on standing. So what do you do now with *Remijas*? You have to get into discovery. You have to get into the facts and depositions. But there are many questions: how do you handle duty, how do you handle breach of duty?

I like to file summary judgment very early in federal cases. So do you now, rather than file a 12(b)(6) motion, file a summary judgment and force the plaintiff to file a motion for discovery? I'm interested to see how it will impact the nuts and bolts of a litigator's strategy, discovery can be a very dangerous thing for many of these companies.

HORNAK: In some respects, the *Clapper* case was also results-oriented, an attempt to protect the federal government from litigation over its surveillance practices. The Supreme Court was looking at a precise issue, and not considering data breach cases and other Article III standing issues.

And now we have *Spokeo*, and we can all vote for what we think the result is going to be. The court might simply say that was an actual damage, not a substantial risk of future harm, and not resolve the issue for us with regard to data breach. It's possible we won't get much guidance in the context of the theft of credit card information.

Regardless, this case could greatly impact class action filings. Right now, class actions get settled because there are questions and doubts about Article III standing: A plaintiff may get beyond the pleading attack, but will class cert. we granted, and will standing be shown through trial? If we get some clarity on that, it's going to dramatically affect the balance.

MODERATOR: On the regulatory side, we saw an interesting decision in *FTC v. Wyndham*. What is the impact of this ruling?

HORNAK: The FTC has taken the position that it has jurisdiction over cybersecurity matters under Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, much like California's Business and Professions Code Section 17200.

In *FTC v. Wyndham*, 799 F. 3d 236 (3rd Circuit 2015), Wyndham wanted to test whether the FTC really did have jurisdiction. The Third Circuit sided with the FTC and said, yes, the FTC does have jurisdiction, and that the requirements of injury do not apply to the FTC Act in the way Article III standing requirements apply in the private context.

Since that decision, I know there have been one or more commissioners in the FTC, who question whether

> One of the things I would recommend to a business of any size is to have good logging of all systems. Because in the event of a suspected breach, you can get a professional to evaluate those logs and possibly determine whether or not you actually had a breach, and if so, the extent of the breach, and whether or not you need to notify someone. Without those logs, you don't really have much of a technical leg to stand on.
>
> **– DAVE WATTS**

> The thing that makes me want to cry following some of these data breaches is that there are so many insurance policies out there, and great add-on options and yet many companies do not obtain coverage. It's like they are barreling down the 405 freeway at 100 mph without a seatbelt. It's reasonably easy to get insured for this risk—much easier than it was five, ten years ago. Now is the time to get a policy.
>
> **– ERIK SYVERSON**

that's the law. The FTC lost one of those decisions and has appealed it, so there remains a bit of an open question as what needs to be shown for the FTC to have jurisdiction; however, if we assume that *Wyndham* represents the law, we are going to see more FTC involvement in the data breach arena. We've seen about 50 FTC proceedings taken against companies just in the last year.

BALLON: Most FTC enforcement actions settle. One of the reasons why is that the FTC is good at issuing press releases that are widely reported. *Wyndham* was a notable exception, where a company decided to take on the FTC. Many companies believe that they cannot withstand the adverse publicity attendant to an FTC enforcement action.

The FTC has very broad jurisdiction under of the FTC Act over unfair or deceptive practices that impact consumers. Its jurisdiction has been supplemented explicitly under COPPA, Gramm-Leach-Bliley, and other acts. But there is also the phenomenon of regulatory creep at play. When I first began work on my treatise in 1995, the FTC was just beginning to study data privacy. By the time the first edition was published in 2000, the FTC's website identified data privacy as central to its oversight function.

In the last few years, the FTC has been more punitive in the settlements that it has been demanding to resolve enforcement actions. To require 20 years of monitoring, for example, in an industry where companies rise and fall in a matter of five years or less is significant.

So we've seen not only that in the past 20 years the FTC itself has greatly expanded its jurisdiction, but in the past six or seven years that the FTC has been much more demanding of companies in terms what the agency requires to settle a case.

SYVERSON: That's very true. I have had cases where we have entered into a consent agreement with 20 years' worth of monitoring. It's quite onerous. I often ask the FTC why they would even want 20 years' worth of monitoring. Can we make it five years? But they will insist on 20 years. They will negotiate on money much, much more easily with the 20 years of monitoring.

RING: This was another aspect of the *Wyndham* decision: the FTC is regulating companies now without having to actually go through the rule-making and administrative process that would otherwise be required. And that was one of the challenges that Wyndham made. Wyndham was saying, "We didn't know what 'reasonable security' meant to the FTC under the Act, so we didn't get fair notice." And the Third Circuit said, "You know how you should be handling credit card information, because the FTC has issued some guidance on this, and there are industry standards on it."

The settlement that Wyndham ultimately reached with the FTC after they lost at the Third Circuit is very clear on what is required. Most consent decrees in data breach cases are boilerplate. But this one goes into a lot more detail about what's required when credit card information is involved.

HORNAK: What the FTC is doing is putting in settlement agreements its idea of reasonableness, and publishing it in consent decrees.

SYVERSON: Right. And whether it's the FTC or a state agency, I find that they tend to get married to one industry, which can make the settlement process a challenge. Healthcare, for example, seems to be the area where regulators have the most expertise. That's where many privacy-based professionals have cut their teeth. And so you try to apply the standards of reasonableness and care from healthcare to another emerging industry, and you end up with a square-

peg-in-a-round-hole situation. It can be tough, from a deal-making standpoint.

MODERATOR: Are there any new developments in the insurance market to guard against data breaches?

SYVERSON: The thing that makes me want to cry following some of these data breaches is that there are so many insurance policies out there, and great add-on options and yet many companies do not obtain coverage. It's like they are barreling down the 405 freeway at 100 mph without a seatbelt. It's reasonably easy to get insured for this risk—much easier than it was five, ten years ago. Now is the time to get a policy.

HORNAK: The policies are all different. So companies have to look carefully at what the exclusions are. For example, some policies contain exclusions if there was participation by employees of the company in the data breach incident. Many of them require lengthy questionnaires about the company's security practices, so they need to look closely. But I think Erik [Syverson] is right, policies are relatively cheap right now, in the same way as when we first had Internet retailers.

WATTS: Another piece of advice is to be honest. Whether it's for first-party insurance or third-party insurance, don't sugarcoat anything on your application, and be absolutely forthright on all of your shortcomings. If you don't know how to answer a question, don't just check "yes." It's better to pay a higher rate and have a claim paid, than to pay the money and have no protection.

SYVERSON: That's true. A few coverage disputes have been starting to crop up in the last year, and they are usually about a company's failure to disclose either a prior breach incident or the level of privacy hygiene. Finally, some parting advice to law firms: get cyber liability insurance, or get ready for major breach liabilities in 2016.