2015 Roundtable Series

Privacy

Law and precedents surrounding data privacy and security are mounting in jurisdictions across the country and around the world, putting conflicting pressures on businesses and their attorneys. Meanwhile, practitioners are advising clients on litigation over data breaches, on how to improve and implement policies for "data privacy hygiene," and on how to insure themselves against cyber risks.

California Lawyer moderated a conversation on these and related issues among Tanya Forsheit of Baker Hostetler; Simon J. Frankel and Lindsey L. Tonsager of Covington & Burling; and Erik S. Syverson of Raines Feldman. The roundtable was reported by Connie Martin Dunne with Barkley Court Reporters.

Participants

TANYA FORSHEIT
Baker Hostetler

SIMON J. FRANKEL
Covington & Burling

ERIK S. SYVERSON
Raines Feldman

LINDSEY L. TONSAGER
Covington & Burling

EXECUTIVE SUMMARY

MODERATOR: Where is this volatile field headed right now?

TANYA FORSHEIT: Well, this year is going to bring changes in California law, including what's sometimes called the "Eraser Button" law (Privacy Rights for California Minors in the Digital World, Business & Professions Code §§ 22580-22582). It goes into effect this month and gives minors the right to have content removed, if they posted it. It's the first law of its kind in the U.S. More generally, we're seeing increased concerns about data collection and sharing and what's appropriate, from legal and ethical and security perspectives. Plus very high-profile security incidents are affecting companies in every sector. It's a whole new era, compared with five or ten years ago. There's almost no industry, no jurisdiction, not even any real legal practice that isn't touched by privacy and security issues.

LINDSEY L. TONSAGER: The California Minors' Privacy law also has marketing and advertising restrictions that create practical challenges for general audience sites that have a difficult time distinguishing between advertising that's delivered to registered teens and advertising that's delivered to registered adults.

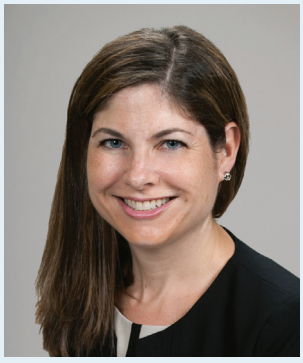
ERIK S. SYVERSON: What strikes me right now is everyday citizens are reevaluating their relationship with the Internet—what they put out there and how it impacts their lives. I get a lot of calls from people whose children have put something out and they can't get it back. You know, all government is local. People are putting pressure on their state representatives, and you see this patchwork of laws. And that's really going to make it difficult to do business on a national scale. It's a constant catch-up game, the legislation process—let alone the litigation process.

TONSAGER: The California Minors' Privacy law was closely timed to the debate in Europe about the right to be forgotten. To the California Legislature's credit, the California law mostly got it right with its exception to accommodate First Amendment concerns by allowing people only to take down content that they posted themselves.

FORSHEIT: Just for the counterpoint, there's other recent privacy legislation where California maybe didn't get it right—the do-not-track disclosure law that kicked in in 2014 (California Business & Professions Code §§ 22575-22579). California said you have to say in your privacy policy how you respond to a do-not-track signal if you engage in that kind of tracking of customers. So companies are just putting up boilerplate statements—and that is about all you can do, really—saying that there's no industry consensus on what this means, so we are right now not doing anything differently when we receive a do-not-track signal, and here's what to do if you want more information. There are some companies like Yahoo that really have made changes (announcing recently it will honor Do Not Track in Firefox), but I think California really jumped the gun.

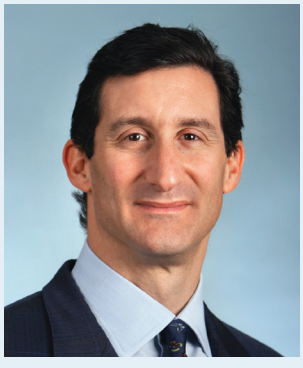
MODERATOR: How's the landscape changing for litigation under the federal Telephone Consumer Protection Act?

SYVERSON: The partner I worked with when I started practicing represented a lot of telemarketers on claims under the TCPA, and I had kind of written it off as a thing of the past. Then in the last year or two there's been an explosion in class actions under TCPA. It's been interesting to see it repurposed in the spam arena. In the Central District alone, I can't think of a day in the last year where I haven't seen a new TCPA action; if you're a business and you want to market using SMS, I think it's, frankly, nuts.



TANYA FORSHEIT advises organizations across disciplines, from multinationals to startups, in compliance, transactions, and litigation involving the use, sharing, and protection of sensitive information, and she serves as outside privacy counsel to several organizations. Tanya brings more than 17 years of experience litigating complex disputes, as well as her cloud computing and social media knowledge, to bear in counseling clients on thorny issues in data management, information protection, and e-discovery.

tforsheit@bakerlaw.com
bakerlaw.com



SIMON FRANKEL focuses his practice on copyright and trademark litigation, technology and Internet privacy disputes, and legal issues related to visual art. He has handled numerous online privacy class actions asserting claims under the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Video Privacy Protection Act for clients such as LinkedIn, Huawei, and Cable One.

sfrankel@cov.com
cov.com

SIMON J. FRANKEL: That's parallel to what we've been seeing for half a dozen years under statutes such as the Wiretap Act and the Stored Communications Act (both part of the Electronic Communications Privacy Act, or ECPA), and now the Video Privacy Protection Act. Legislators, like the rest of us, are often fighting the last war, so it's not surprising that they're doing a better job of looking backward than forward.

SYVERSON: Piggybacking on that, the idea of repurposing statutes or applying them in new landscapes has made them real weapons. Take cases like *Larocca v. Larocca*, which really is just a divorce in a family court. With the addition of satellite litigation in federal court, couples are now able to use ECPA as a weapon against each other. (See *LaRocca v. LaRocca, 2014 WL 5040720 (E.D. La. Sept. 29, 2014).*)

FRANKEL: Similarly, the Computer Fraud and Abuse Act is being applied in what used to be basic trade secret cases, where you asked, "Did the person take information that he or she shouldn't have and use it with the new employer, and was that permissible?" Now, the question is, "How did the former employee take that information—was it from a computer without authorization?"

TONSAGER: Data has become another business asset. So you see companies trying to use their internal privacy policies and privacy laws to proactively try to protect that asset, along with confidential trade secrets and other proprietary types of information.

MODERATOR: What are the implications of that for data breaches?

TONSAGER: You have a companywide policy that says, "We are going to allow our employees to access only data that they need." You have a data retention policy that says, "As soon as we don't need data we're going to delete it." Those are both strong privacy policies, but they have incidental benefits that flow through the company, including protecting proprietary trade secrets and other business data from breaches.

FRANKEL: And correlating with that is the need to actually follow those policies.

FORSHEIT: We certainly see a lot of situations where people want to try to get something on paper but it can be purely aspirational, which it should never be, of course, and that can really create a problem. Good data privacy practices are really about information governance, and not just personally identifiable information but company confidential information, trade secrets, intellectual property—all of that.

FRANKEL: That turns out to be incredibly important when you're arguing in litigation, as almost all these statutes allow you to, that your users consented to this particular use of this particular information. If you have a good policy that sets out clearly what specific uses you are making with particular data and have sought and obtained users' valid consent to those uses, that's often a terrific position to be in. What you don't want is to go beyond that, as in the comScore class action, *Harris v. comScore, Inc.*

SYVERSON: Part of the issue is that these are really dynamic companies, often being driven by very dynamic, young people, and they're going through very rapid changes. I've met with companies right before they've gotten much, much larger and gone to a national scale, and you can see a problem on the horizon and they don't address it and, a year later, I read about the class action against them. That's when you say, "Oh, yeah, I hope they're insured."

FORSHEIT: We're talking about Big Data. What's happening is—whether the company is new and a startup and trying to do something that's new and edgy, or it's old-school—many companies are finding themselves in possession of huge troves of data from customers or employees or whatever source. Consumers really want what they want when they want it—until I go on Facebook and see ads about the place I went on my rideshare or the item I was shopping for on Google. Consumers, at least in this country, are conflicted, and that creates a dilemma for legislators and companies. In Europe, there's more awareness and the culture of privacy has been there for a longer time.

MODERATOR: Let's take that to the Internet of Things, where a machine can know

so much about you. Is there any significant litigation yet? What kinds of limits are going to arise?

TONSAGER: In the next few months, the Federal Trade Commission is expected to outline its nonbinding legal guidance about the Internet of Things. The agency likely will focus on two issues: privacy notices and data security. How do you give people notice about how the device is gathering all this information, using it, and disclosing it, particularly when the device doesn't even have a screen? And how do you ensure that data isn't being accessed in unauthorized ways?

The Federal Trade Commission does seem to recognize the societal benefits that these connected devices have. Think about a medical device collecting information about the medication you're taking, the doses, the frequency. Hopefully, the report will allow innovation to occur while also ensuring that people's privacy is protected.

SYVERSON: Looking at it from a consumer's angle, I think privacy ultimately loses, if we play it out. I really don't think people care about privacy. There's a vocal core who do, but your average Joe 24-year-old on the street doesn't care because they've grown up sharing everything about their life with everyone else.

TONSAGER: I respectfully disagree. There are some great studies by people like Dana Boyd at Microsoft Research showing teens, in particular, doing incredible things to protect their privacy, such as deactivating their social media accounts each day to prevent their parents from seeing what they're posting. It's just that young people are very creative and are coming up with different privacy norms and solutions.

FORSHEIT: Yeah. I don't think we would have seen all the consequences from the Snowden situation if Millennials did not care about privacy. In many ways, the younger generation is more concerned about data getting into the hands of the government, which itself raises some interesting questions, which is why are we demonizing what the government is doing but perhaps not as concerned about what the private sector could do.

MODERATOR: What are the issues you see coming up for consumers who aren't thinking about privacy?

FRANKEL: Well, one obvious answer is the recognition in the last few years by many people that everything they do online—whatever they post, whatever images they send—could come up later in their life when they apply for jobs, or apply for college.

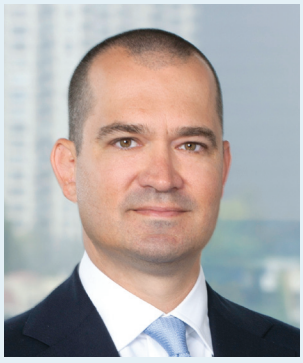
FORSHEIT: McAfee and some other companies are trying to educate young people -- teenagers and even younger -- about the risks of online behavior. I think education has a bigger role to play than the legal system in preparing that generation.

SYVERSON: I guess I'm taking the viewpoint that data is money, and data is the currency of the Internet. It's tradeable so the monetary incentive will just trump privacy. People want convenience, and the tradeoff for that is to give us your data and trust us with it.

FRANKEL: I'm not convinced. There are a lot of emerging technologies to provide equivalent services at some small cost with greater privacy protections. We'll have to see whether people care, but there's scholarship on the "cost of free" in this fundamental grand bargain where you trade your information for free online services. And it may just be that different market segments will emerge where some people make different choices, to pay a little, to have different terms of use with a little more privacy.

FORSHEIT: It's worth mentioning that privacy as a product itself raises a lot of issues. We saw a recent FTC settlement with TRUSTe, the privacy seal organization. It didn't have to do with TRUSTe's own privacy practices but whether the company had been monitoring and vetting the companies it certifies as regularly as it should have been. So privacy as a product becomes very circular. I have clients who are saying, "What's the value of a TRUSTe seal now, and what's the alternative?"

SYVERSON: There are professional versions of SnapChat that market to law firms. It's a visceral communication; it disappears, and that's becoming the selling point that's being marketed to law firms to interface with clients.



ERIK SYVERSON is a partner with Raines Feldman in Beverly Hills. He leads the firm's Internet and digital media law practice. In addition to intellectual property and defamation actions, Erik and his team frequently defend small to mid-market companies in data breach and privacy suits. Typical cases involve claims under federal and state privacy statutes including the Computer Fraud and Abuse Act, the Stored Communications Act, HIPAA, and various negligence-based theories.

esyverson@raineslaw.com
raineslaw.com

LINDSEY TONSAGER represents clients in policy proceedings and investigations by Congress, the Federal Trade Commission, and other regulators. She helps clients develop strategies for complying with laws governing student and children's privacy, behavioral advertising, email marketing, endorsements, and new technologies. She advises clients on mitigating the risk of unauthorized disclosure of confidential information and in developing clear privacy notices and policies.

ltonsager@cov.com
cov.com

FRANKEL: I'm not sure I would want that.

MODERATOR: What is the FTC doing with regard to children's privacy?

TONSAGER: It has made good on its promise to make children's privacy a priority, and it seems to be applying a carrot-and-stick model. It recently rejected AgeCheq's application for a verifiable parental consent mechanism, which really was a carrot because it reasoned AgeCheq didn't need approval--it was already permitted under the Children's Online Privacy Protection Act.

Examples of "sticks" are recent enforcement actions against Yelp and TinyCo. Yelp, which is a general audience app, has a registration flow that collects age information, and it was letting children register. What's interesting is Yelp actually tried to comply with COPPA, but the third party it used to check compliance allegedly missed the fact that children were registering. The FTC didn't give Yelp a break. In the TinyCo case, the FTC alleged the company did not appropriately provide parents notice or gain parental consent for collecting email information. Both companies settled the cases, paid civil penalties, and agreed to ten-year consent decrees.

MODERATOR: What kinds of litigation risks do companies face when they disclose customer information to their business partners?

FORSHEIT: In the Target data breach, the guys got in through an air conditioning vendor. So you have to wonder what it means for companies to share information and how that increases their risk. A lot of it has to do with doing significant due diligence as to vendors and service providers. Not treating it as a check-the-box exercise is key, and those companies also have to involve information security professionals. Stakeholders need to say what information they really need to share, and determine whether each vendor's security matches their own.

MODERATOR: So is there a business interest developing in privacy?

SYVERSON: Yes, but it's hard to advise clients in a space that changes so rapidly. Something you might say they'd be nuts for serving today could in two years become the norm. We can go on and on with examples, but when YouTube started, you'd say you're just asking for infringement suits. Now, I'm a sports nut so I consume a lot of sports content on YouTube, and there's a lot of copyrighted content there, and it seems to have become the norm.

MODERATOR: What are the legal implications of the way that major recent breaches have been handled? Just to name a few: Adobe, Target, Home Depot, Sutter, JP Morgan, Sony.

FORSHEIT: The standards for how companies must protect information are a moving target, but the FTC and the courts are looking to what is common in your industry, in your particular sector and finding whether there were basic things you should have been doing: encryption, dual-factor authentication, and so on. But in some situations a company could not have done more.

TONSAGER: There's tremendous uncertainty because of litigation that's going on right now between the Federal Trade Commission and Wyndham and LabMD, where the FTC is alleging that these companies didn't employ reasonable data security practices; there are no specific legal rules, but the FTC is claiming, "You should know what's reasonable based on a speech that an FTC commissioner or staff member gave or our guidance documents that we're posting on our website." That's not a clear standard.

SYVERSON: These cases are very interesting. Yes, consumers are going to lose out because of problems with causation and damages. But with the Target and Adobe cases, negligence theories are starting to evolve where, once they can get past a Rule 12b6 motion, you could be looking at huge damages. I think you'll see the language the judge used in the Target case in establishing a duty of care to banks emerge in the consumer context also.

Just investing in your data security may be the best insurance of all if these negligence theories emerge. Then you can say, "We hired the best. We have the best technology." That might be your best defense. But it's just as important now for the smaller players to insure themselves as it is for the Googles and the Yelps. If you have a data breach, it could just wipe you out—and insurance is required by a lot of counterparty contracts now.

FRANKEL: I'm not sure we will see a lot of successful data breach cases. In these class actions, the classes often have been protected by credit monitoring provided by the defendants, and there's been this real question of what harm plaintiffs suffered. There's a distinction between data breach class actions where people are claiming breach of contract or negligence versus online privacy cases where there are statutory claims that may offer statutory damages. But ultimately, it may be that the real action in the data breach arena is at the regulatory level in terms of what kind of proceedings companies are going to be subject to by state and federal government, and then in the marketplace, in terms of the way suffering a data breach will affect how a company is perceived by consumers.

TONSAGER: One practical takeaway from these data breach examples is that, for a long time, in-house lawyers who deal with privacy compliance really struggled to make a business case to their executives for their existence. Saying, "You can't do this, you must do that" to protect data was not always looked upon well within a company. Now, not only do you have privacy lawyers helping protect data as an asset, but you have these examples where executives are losing their jobs because consumer data or employee data is breached. And that's providing in-house lawyers an opportunity to really demonstrate their value. ■