NEW YORK METRO / 2013

Super Lawyers®

SUPERLAWYERS.COM

MAGAZINE

THE ANNUAL LIST

The Top Attorneys in the New York Metro area

INCLUDING RISING STARS

The Queen of Breach

Privacy expert Lisa Sotto goes public

BY RAY PHILLIPS
PHOTOGRAPHY BY MICHAEL PARAS

THOMSON REUTERS

LISA J. SOTTO

- MANAGING PARTNER OF THE NEW YORK OFFICE, HUNTON & WILLIAMS
- INFORMATION TECHNOLOGY/ OUTSOURCING
- NEW YORK METRO SUPER LAWYERS: 2006–2013

IN 2004, NIGERIAN FRAUDSTERS POSING AS small-businessmen opened bogus accounts with ChoicePoint Inc., an aggregation company that gathered massive amounts of personal data and then sold access to its database to businesses and the federal government. The fraudsters obtained tens of thousands of names and other personal information, but the real sticking point was what happened once ChoicePoint became aware that its data had been compromised: It notified only California residents. Only California had a data-breach notification law. A public outcry followed, leading to the first widespread adoption of data-breach notification laws, which compel companies to notify victims of a breach.

"ChoicePoint looks quaint compared with what came later," says Lisa Sotto, head of Hunton & Williams' privacy and cybersecurity practice, who also chairs the U.S. Department of Homeland Security Data Privacy and Integrity Advisory Committee. She is also the lead author on *Privacy and Data Security Law Deskbook*, published in 2010 and frequently updated, which is considered by many to be the Bible on data privacy issues.

"We have gotten to a point where the information that is out there about us controls our lives," Sotto says. "If your date of birth is wrong or a digit on your Social Security number is transcribed incorrectly, you can be denied a job, turned down for government assistance or a grant, or kept from getting on a flight."

Hunton has worked with clients on more than 900 information security breaches. From the firm's perspective, this generally involves the initial investigation of the breach; examining the client's relevant contracts, insurance and applicable breach notification laws; working with law enforcement; aiding in the legal notification of victims; and handling any subsequent litigation. The firm also undertakes the crucial work of reputation management. It's not a hurry-up process.

"Forensics investigations alone can take months, identifying the scope of the security issue," Sotto says.

Most data losses occur inadvertently and are not the result of malicious behavior. But whether data is misplaced or stolen, there are potentially ruinous consequences for both the individuals affected and the company responsible for safeguarding the data. Although companies are now bound by law to report data breaches and typically try to remedy them, that's often small comfort to the individual who today has little choice but to share personal data online.

"As a Secret Service agent told me," Sotto says, "each of us can only pray our information is that needle in a haystack nobody ever finds."

SOTTO'S CORNER OFFICE ON THE 51ST FLOOR of the MetLife Building is an appropriate perch from which to keep an eye on the evolution of data privacy law—her closest neighbors are snooping griffins atop the Chrysler Building. The office is filled with photographs of her family: teenage daughters Rebecca and Arielle, 6-year old son Shane, and husband Bruce Saber, a leading real estate attorney with Arnold & Porter. Their home is only 10 minutes away. That proximity, she says, is essential given her demanding schedule.

"This is a full-time *plus* job," she says. "I'm often in the office until midnight. Weekends are sacrosanct for family, but the beauty of living so close is that even midweek I can participate in school events."

Playfully dubbed "the Queen of Breach" by one client, Sotto is known widely as a data privacy expert. "She conveys a sense that you are going to get a consistently right answer at any time of day," says a client. Adds colleague Monika Jedrzejowska, "Every minute she has between meetings and calls she scans the privacy publications, to make sure she is up on the latest developments." Aaron P. Simpson, a Hunton partner and Sotto's protégé since 2004, says, "I believe the key to her success is her dedication to client service. She's the single most loyal and relentless advocate I have seen in my legal career."

A native New Yorker, Sotto grew up in Riverdale and attended the Bronx High School of Science. At Cornell University, she majored in history, focusing on American Colonial history, and during college spent a semester in Washington, D.C. She loved studying history but since childhood she has loved to solve problems and interact with people. "There was no deviation," she remembers. "I was going to law school."

After graduating from the University of Pennsylvania Law School in 1987, she began working in environmental law and joined Hunton in 1989. Then in the late 1990s she became interested in new technology: the Internet.

"Here," she remembers thinking, "you had this unprecedented gathering of information, with a corresponding lack of clarity about who controlled access to it." The head of Hunton's technology practice, uninterested in retraining her as a corporate lawyer, did point her in the

"As a Secret Service agent told me," Sotto says, "each of us can only pray our information is that needle in a haystack nobody ever finds."

In 2012, Sotto (here with USAID rep Benjamin Allen and two Serbian nationals) was invited to Belgrade to assist the Serbian government in upgrading its data privacy laws.

direction of privacy law, which soon seemed likely to require the kind of comprehensive regulatory development U.S. environmental law had gone through in the 1970s and 1980s.

"I've always been struck by the many analogies between environmental and privacy law," she says. "One worries about the collection of data from cradle to grave much as we think about hazardous material: how to use it, how to store it, and where does it end up at the end of its life-cycle. We talk about data leaks, data flows, data hygiene. But while environmental law was fairly mature by 1999, for data privacy there was virtually nothing."

Her firm, she says, went "whole hog" with its data privacy practice. "We got in this first. It was a gamble, but we perceived that information would itself become an asset, so it was a good gamble. Today there are many imitators. ... [But] with our experience on over 900 data breach cases, and our global reach, no one else comes close."

Within two years of Hunton launching the practice in earnest in 2000, privacy became 100 percent of Sotto's practice. "We hired a privacy lawyer in Brussels," she says, "because Europe was so far ahead of the United States in this area—in 1995 they had devised the European Data Protection Directive, with the member states of the EU enacting the directive into local law—and from there the dominoes just fell. We now have 10 attorneys and a paralegal on our privacy and cybersecurity team in NYC, and we have seven to eight data protection lawyers [each] in London and Brussels, because we need people at the epicenter. Meanwhile, the head of our Beijing office has been working on Asian data protection issues since 2005."

Sotto distinguishes what Europe's omnibus directive means. "In America we have a sectoral regime, meaning we regulate privacy by industry sector or type of data. There are laws for financial data, health data, data collected online from children under 13, drivers' data, and so on. But in that sense we are out of step with the rest of the world. What this means for the global businesses that are our clients is that they have to jump through hoops to assure compliance with a diverse set of international rules."

Even so, she insists that unifying global action on data protection cannot ignore varying cultural norms.

"People think of privacy differently in Indonesia, in the UK, in Poland, in Venezuela, around the world," she says. "The Europeans have a history of despotic regimes: the Nazis, Tito in Yugoslavia, and secret police like the Stasi in East Germany. The use of personal data in lists and dossiers to persecute people is still very fresh in their minds. In the U.S. we typically think of privacy as a consumer protection interest. Our primary regulator for privacy is the FTC—the Federal *Trade* Commission. Overseas, the protection of personal information remains a fundamental human right."

Of course, the concept of information privacy has been challenged in recent months with the revelation that the NSA has been collecting broad swaths of phone records and information about Internet activities.

"The media has boiled the issue down to privacy versus national security, but we shouldn't have to choose one over the other," Sotto says. Then she lists off the questions that need to be asked. "Who has access to the data? For what purpose? How long are the records maintained? What's the process for vetting potential new uses of the data following the initial collection? How is the data secured? No matter how well-intentioned today's leaders are in using the data only to fight terrorism, having such massive digital databases can tempt future leaders who may have different intentions."

THESE DAYS, DATA PRIVACY ISSUES ARE increasingly overshadowed by the threat of cyberspying, which defense experts recognize as a new form of warfare, in which a foreign entity invades U.S. cyberspace for purposes of espionage or sabotage. Nine years ago, Sotto was selected to join the U.S. Department of Homeland Security Data Privacy and Integrity Advisory Committee; today, she serves as its chair. The committee advises the secretary of Homeland Security on data privacy issues, and its members prepare reports that inform the department's activities.

Sotto takes pride in the cybersecurity-related work she's done for the private sector, assisting in efforts to combat all manner of cyberthreats to the nation's financial networks, telecommunications and high-tech services, credit card systems, and other private businesses.

The frequency of these attacks is growing, often targeting the U.S. military or leading energy and aerospace firms, climbing from 50 reported attacks per week in 2010 to 102 per week in 2012. Meanwhile, hacktivist groups commit website defacements, steal data, or create denial-of-service attacks to shut down or slow Internet service.

"Spying has been done since time immemorial," Sotto says. "But now everybody has a computer, so cyberespionage has the potential to affect everyone. And the law hasn't kept up with the threat. When a hacker steals Social Security numbers to commit identity theft, the organization that was hacked must notify and assist the people whose data was compromised. But who does a company turn to when business secrets are stolen? Who can help? ... Only government agencies like the FBI, the Secret Service and DHS can connect the dots when several businesses are attacked by the same hacker. But for most companies there's no mandate to report cyberattacks. And there's no legal regime in place, no playbook for handling these situations."

Sotto, who has testified before Congress on these issues, feels the sense of urgency, and regrets that at present companies who experience hostile invasions are largely left to fend for themselves.

"It's an ongoing struggle, and we don't have all the answers," she says. "We're only 20 years out from the introduction of the World Wide Web and the future continues to advance at lightning speed—smart phones, wearable computers, cloud computing—all of these evolving technologies present data privacy and security issues. It's all gone so fast, which is why the law is struggling to keep up. We're just starting to understand the parameters of the issue and just starting to talk as a larger society. We are not there yet." SL