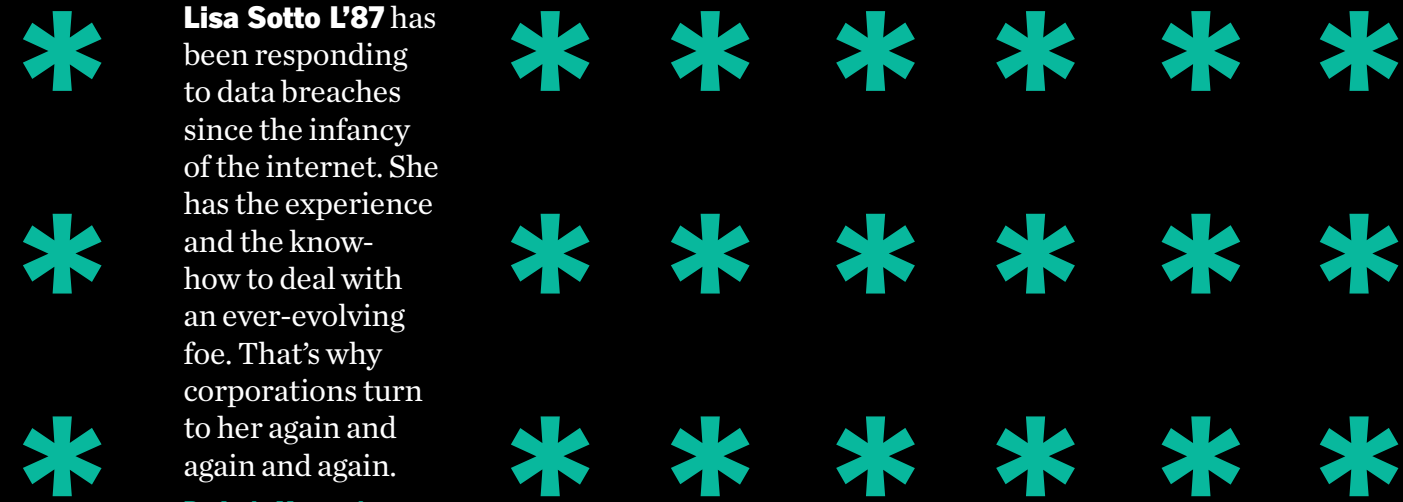


\* \* \* \* \*  
\* \* \* \* \*  
\* \* \* \* \*  
\* THE \* \* \* \* \*  
P R I E S T E S S S  
\* O F \* \* \* \* \*  
P R I V A C Y \* \* \*

**Lisa Sotto L'87** has been responding to data breaches since the infancy of the internet. She has the experience and the know-how to deal with an ever-evolving foe. That's why corporations turn to her again and again and again.

By **Andy Maynard**







Former CEO of Yahoo Marissa Mayer after a hearing before the Senate Commerce, Science and Transportation Committee. Yahoo suffered two monumental data breaches several years ago that cost the company mightily and caused policymakers to review outdated privacy laws. Cybersecurity expert Lisa Sotto L'87 represented Yahoo, working nonstop to quell the crisis.



In 2013 and 2014 two data breaches, or the unauthorized acquisition of personal information by malicious parties, occurred at Yahoo. Over time, hackers (including state-sponsored intruders) were able to gather user account information on a scale never before seen in the short lifespan of the World Wide Web. Not info on thousands of users, not hundreds of thousands, nor even millions — more than three billion user accounts were affected. That is almost half the world's population. By the time the events were detected and made public in 2016 and 2017, the consequences were far-reaching — \$350 million was knocked off of Yahoo's sale price to Verizon, lawsuits were brought against Yahoo, and policymakers rushed to review suddenly-outdated privacy laws.

In the middle of that maelstrom calmly stood Lisa Sotto L'87, who, drawing on years of experience in the arena, was brought in to quell the mounting crisis. Working nonstop, she provided advice on the mammoth task of contacting affected users and on handling the inevitable legal complexities.

While it was far from another day in the office, it was vintage Sotto, who heads the global privacy and cybersecurity practice at Hunton Andrews Kurth and serves as managing partner of the firm's New York office.

To hear her clients tell it, no one is better at putting out these kinds of five-alarm fires than Sotto.

"You can't practice in this area and not know Lisa."

"At the very top of experts in the field."

"Unquestionably the industry's leading professional."

And, finally:

"The high priestess of privacy."


So how did Lisa Sotto find herself in such rarified air, at the very top of the data privacy field? It all started at Penn Law, where as a 3L student in 1986–87, she had different plans. "I did [have a plan], but it didn't work out that way. I was a dyed-in-the-wool litigator, and absolutely planned to be a trial attorney," Sotto says. She graduated from Penn Law in 1987 and became an associate at Cadwalader Wickersham & Taft in New York City. At the time, the firm had a rotation program for young lawyers that acclimated them to various aspects of the firm. She spent her first year splitting time between the litigation and corporate groups. It was during this program that Lisa discovered a new interest in environmental law.

Shifting gears, she quickly got up to speed on regulatory rules, and it was as an environmental lawyer at Hunton & Williams (now Hunton Andrews Kurth) where she would discover something that would change her life forever—that many of the same rules and best practices of environmental law applied to the still embryonic field of data privacy. "It required a very short transition period," Sotto says. "If you think about the two areas, they're actually very similar. They are areas of regulatory law, so you deal with regulatory compliance. You're tangling with executive agencies like the EPA (Environmental Protection Agency) and FTC (Federal Trade Commission). We talk in the privacy world about data breaches, or data leaks—not so different from hazardous substance leaks."

Back then, the notion of data privacy was far different than how we view it today. Computers and connectivity were still in their infancy, and the idea of privacy law was quite different. "We didn't have any shared sense of what privacy law was," said Keith Enright, chief privacy officer for Google. "When I took a class on privacy law in law school, they were focusing on *Roe v. Wade* and a woman's right to choose. They were not thinking about data protection in the way that we think about it now."

"It was a wide-open field when I started in it," says Sotto. When she expressed interest in privacy law, she got the approval of the head of the Technology group of the firm. "He sent me the entire compendium of U.S. privacy law at the time, which was probably 1/16th of an inch. It was very light—there was nothing there. It was easy to become an 'expert' after a couple of hours of reading."

By the end of the twentieth century, however, two major technological trends were converging—computers were becoming faster and more powerful, while more and more people were connecting to the internet. Meanwhile, privacy laws were lagging behind these developments, and very few individuals grasped the relationship between technology and data privacy. But one of those people was Lisa Sotto, who had switched from environmental law to data privacy law at Hunton. Before long, she had thrown the 1/16th inch rulebook out the window in favor of her own.



**“THE FIRST  
24–36 HOURS  
ARE CRITICAL.  
OFTEN WHEN  
[LISA] GETS  
THE CALL...  
VERY LITTLE  
IS KNOWN  
ABOUT THE  
NATURE AND  
SCOPE OF  
THE INCIDENT.”**


BRITTANY BACON, *Hunton Andrews Kurth*

Since then, Sotto has meticulously built her practice from scratch. Her clients have included six of the ten largest corporations in the country, among them companies that have suffered data breaches as well as those who are preparing for the worst. Mock data breaches and tabletop exercises (wherein you simulate an attack and develop a response) are conducted so that organizations will know what to do in case of a data security emergency.

Data breaches are typically carried out by nation-states capable of sustained, advanced attacks; “traditional” hackers interested in finding something to sell on the dark web (the unindexed part of the web that is difficult to find); and hacker activists, or “hacktivists,” who attempt to bring down a website or steal information in order to embarrass a company or promote a cause. One of these groups will find a way to exploit a weakness or unintended aspect of a program, a backdoor into a network, or use “phishing” techniques to gain access to an otherwise secure system. Once inside, they can stay hidden for days, weeks, or even months. In about half of all data breaches, the company itself does not detect the breach, but is notified by a research company, the media, or the FBI.

Once a breach is detected, companies must decide quickly how to act. “The first 24–36 hours are critical,” says Brittany Bacon, a partner on Sotto’s team at Hunton. “Often when [Lisa] gets the call from the general counsel, the chief information security officer (CISO), or the chief privacy officer, very little is known about the nature and scope of the incident.” For companies operating under the new data privacy law in Europe, the European Union’s General Data Protection Regulation (GDPR), they have 72 hours to issue breach notifications to regulators, even though the company itself is still stuck in a fog of uncertainty and confusion. “You have an organization that has often times suffered an adverse event, and is investigating, gathering facts, trying to make sure that they understand precisely what happened. They’re also trying to make sure that they’ve addressed whatever vulnerability may have existed and been exploited. That’s creating urgency and drawing people’s time and attention. In parallel, you’re trying to make sure that you’re doing the right things to satisfy all of your legal obligations and mitigate legal risk to your clients,” details Enright. And that’s where Sotto comes in.

Hunton has contacts with external forensic investigators that they can bring in to attempt to identify what was done, by whom, and for how long. “We’re seeking to understand the facts as we’re uncovering them. It could mean we need to conduct a legal analysis of laws around the world. If a big database is compromised, we will reach out to local counsel in various countries where people are impacted,” says



**“DATA IS LIKE WATER, IT DOES NOT RESPECT STATE OR COUNTRY BOUNDARIES. WE CAN NEVER JUST THINK ABOUT THE U.S., WE HAVE TO THINK GLOBALLY.”**

LISA SOTTO - *Hunton Andrews Kurth*

Sotto. This worldwide response often requires many individual steps—gathering evidence, notifications to regulators and affected individuals, press releases, employee talking points, business partner talking points. Sotto knows many of the relevant regulators and will liaise with them on behalf of her client. She also works with PR firms before media outlets get word of the breach. And then, after all of the above, the lawsuits start. On average, the entire process can last two to three years.

“She brings an extraordinary blend of competence and confidence,” says Tom Vandervoort, senior VP and deputy general counsel at Under Armour. “When she walks into a boardroom to brief the board, she owns the room. There’s no question that she knows what she’s doing. She just has that gravitas about her.”

Google’s Keith Enright agrees: “Lisa’s even-handed, balanced, measured approach to giving risk-calibrated advice not only allows a client to meet their

legal obligations but also reassures them that, upon following legal advice, they're doing the right thing. They're going to make it through the current crisis intact. A sort of quiet confidence that she brings to her practice that I think is extremely reassuring to her clients—that is a large measure of her success."

Sotto has assembled a top-notch team at Hunton. It includes 35 people across the globe and a privacy think-tank called the "Center for Information Policy Leadership." This handpicked group—many of them young lawyers—has a wealth of experience in the various aspects of data privacy law and at local, national and global levels.

Many of them joined the team as young lawyers, gradually gaining experience in tense, high-risk situations. According to Vandervoort, "Those lawyers won the professional lottery by ending up on her team. I would go and work for her. I've been at this for almost 30 years, and I would go and work for her.

"She's trained her team in such a way that they have the same type of pragmatism to what they do, and it's not all lockstep or by-the-book because there's so much risk and judgment applied in a moment like that. To impart that risk-taking to younger associates, to younger lawyers, is a real talent."

However, one talent that the newcomers to Lisa's team might not be able to match is her legendary energy level and ability to take calls at all hours of the day. "This is a 24/7 job, sometimes a 25/8 type of job," according to Bacon. "Yet Lisa is the first one to jump when work needs to be done and a client's needs need to be addressed."

"I'm convinced that Lisa doesn't sleep most nights," says Vandervoort. "I don't know when that woman rests. I know how busy we kept her!"

For Sotto, this comprehensiveness, this responsiveness, this global outlook on the industry—all of these are key parts of the job. "One of the biggest challenges in the practice is that you can never rest on prior experience because the field evolves so quickly. We need to stay right at the forefront and keep learning because not only are the threat actors evolving quickly, but also issues involving data and the law are changing at warp speed. Constantly. It is a 24/7 endeavor to try to keep up, and it's global. Data is like water, it does not respect state or country boundaries. We can never just think about the U.S., we have to think globally."

In light of the massive numbers involved in data breaches, can anyone be truly safe from having their information stolen? Given enough time, will a hack or a breach happen to anyone? "To the extent that you have a persistent adversary, absolutely. You just try to be a needle in a haystack, and particularly that needle that nobody's interested in," Sotto explains. "There's

no industry sector that's exempt, nor any individuals, short of those who live off the grid. Remember also that we're not just talking about the internet, we're also talking now about the internet of things. Connected security cameras, connected TVs, connected refrigerators. Just about everything now is hackable."

Companies and individuals can take measures to make themselves that uninteresting needle. A good incident response plan is key—letting people know what they should do in the event of a crisis, their roles and responsibilities. Tabletop exercises and breach drills are very important to build up what Sotto calls "muscle memory." Security policies and processes should be changed frequently to keep up with evolving threats. Individuals and employees must be aware of the dangers of phishing and watch that they don't inadvertently give away vital security information.

As we've seen time and time again through history, however, when under constant threat even the most secure fortress cannot repel all invaders. All it takes is one mistake for the strongest walls to come down—even electronic firewalls. When that happens, there's Sotto. She and her team are a necessity in an age where personal information is transmitted and stored countless times per day. When Yahoo had to face the aftermath of its data breaches, she was the first one upper management called.

"I don't know of any other lawyer or firm who has had more significant experience in [data breaches], or dealt with [these] types of high-profile breaches," says Dan Tepstein, head of litigation, copyright, and media law for Verizon Media, and who was at Yahoo when the breaches occurred. "You're dealing with people who know what they're doing, who have dealt with this in a crisis mode before and can provide the company with the type of leadership and advice that shouldn't be second-guessed."

"The Yahoo matter was probably the pinnacle of my career," says Sotto. "And I say that knowing there could well be something else to follow."

To reach that pinnacle, Sotto has taken a few unexpected turns in her career, going from litigator to environmental lawyer to pioneering leader in cybersecurity, ultimately transforming the once-unknown field of data privacy. She looks back at Penn Law as a formative experience in shaping her life. "Penn didn't have classes on [data privacy]," she says. "But Penn certainly taught me how to be a flexible and practical lawyer. What I've learned is that you have to be nimble as a lawyer, and you shouldn't get fixated on a particular area. Careers change and practice areas morph, and Penn prepared me well for that." ♥

**Andy Maynard** works for the Development & Alumni Relations office at Penn Law. He has fond childhood memories of green monochromatic monitors, loud hard drives, and the noise of a 56k modem.