THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp

Oregon AG Seeks Tougher State Breach Law


By Divonne Smoyer, CIPP/US
Christine Czuprynski

State attorneys general (AGs) are regulators with varying enforcement priorities and policy agendas, even within a focused issue such as data privacy and security. Over the last year, *The Privacy Advisor* has interviewed a number of state AGs who are active in privacy to gain insight into their views. In this spotlight, we talk to Oregon AG Ellen Rosenblum about her work in privacy, including her focus on protecting children online, and her interest in seeing her state's data breach notification law strengthened.

Oregon Attorney General Ellen Rosenblum

The Privacy Advisor: You recently have sought to amend the Oregon data breach notification law to require notice of breaches to your office and to give your office authority to enforce the law. You also have said that the definition of personal information in the law, subject to loss notification, should be

expanded to include medical and biometric information. Are these amendments necessary to keep up with the evolving nature of cyber crime and identity theft? If your office is given enforcement authority, what, if anything, will change in the day-to-day investigation of data breaches in Oregon? If the law is changed to require notification of data breaches to your office, will you follow some other states and make that information publicly available on your website?

Rosenblum: Our current law was written in 2007. Back then, only if you worked somewhere like the Pentagon would you need your fingerprint to open the door. So much has changed in the past eight years. Now, we use our fingerprints to unlock our phones. The dramatic increase in the retention of biometric information presents a particularly serious type of potential breach. You can change your username; you can change your password, but you cannot change your fingerprint. Medical information is also highly sensitive and personal, and with so many different apps and other Internet-driven services collecting this information, we wanted to make sure our laws are updated to better protect Oregonians. But the main purpose of our data breach law is to make sure companies give notice of data breaches in a timely manner and to have reasonable security standards in place. Oregonians deserve to know that if their information is breached they will learn about it promptly and be protected.

If given additional enforcement authority, we would be able to better participate in multistate data breach enforcement actions. These are typically coordinated through the National Association of Attorneys General, and they often join together to coordinate a response when a data breach extends across multiple states. Right now the Oregon state agency tasked with enforcement in this area cannot fully join these actions as an equal partner, so

enforcement of our statute is more difficult than it should be. The Oregon Department of Justice also has very effective tools to gather information about the scope of a data breach and obtain civil penalties for violations.

We already have a searchable online consumer complaint database that tracks consumer complaints, so we hope to make future information on data breaches available through that existing system.

The Privacy Advisor: President Barack Obama recently proposed the Personal Data Notification & Protection Act, which includes a national data breach notification standard. The proposal preempts state law, at least as to laws on computerized records, but gives enforcement authority to state AGs in addition to the Federal Trade Commission. Given your interest in strengthening Oregon's own law, are you in favor of a national breach notification standard? Are there changes to the proposal that you would like to see implemented before it reaches a vote?

Rosenblum: On the one hand, a uniform national law makes a lot of sense here. A lot of the breaches have been nationwide in scale, and industry certainly feels that complying with dozens of different standards is cumbersome. Having a uniform standard would certainly be more efficient. On the other hand, I am concerned that a federal proposal might not be as robust as the better of our state-level statutes. If I could change the law as I understand it, I would allow for filing in state court, recovery of attorneys' fees and a clarification that states can keep any civil penalties awarded. Without those changes, it might be difficult for state AGs to justify bringing an action. Oregon also has a somewhat unique standard that New York is looking to adopt; it clarifies that those collecting personal information have a duty to keep

that information secure. I would hope that any national standard would include that as well.

The Privacy Advisor: You have focused some of your privacy work on protecting children and young people online. Of note, you hosted a symposium in June 2014 entitled “Protecting Oregon Consumers and Children in the Age Of Big Data.” Why are children and young people deserving of special attention?

Rosenblum: One of our priorities at the Department of Justice is to protect our most vulnerable consumers, and this includes children and young people. One thing that came up repeatedly during our symposium is that technology is fast, but the law is slow. If we do not take the time to shape our privacy laws now, I am concerned that any real privacy protections will have little chance of surviving our generation. In keeping with this, one of my highest priorities at the Oregon legislature is the Oregon Student Information Protection Act, Senate Bill 187. After combing through dozens of privacy laws around the country, we decided to start with the thousands of K-12 students in the classroom. This bill is modeled after California’s Student Online Privacy Protection Act, and puts basic, common-sense sidebars around how educational technology providers can use student information collected through their services while generally prohibiting that information from being used for marketing. A very important aspect of this law is that it embraces the Privacy-by-Design model by requiring the educational-technology providers who provide these services to include privacy protections in their product design, rather than requiring school districts, parents or students to opt out or take other affirmative steps to protect themselves. We have seen that the “opt-out” model often leads to long privacy policies that are frequently ignored. Many of our schools don’t have in-house privacy experts who can

help them navigate these very complex contracts, so it's important to put these protections in the statute.

I also introduced Oregon Senate Bill 188, which combats what is commonly called "revenge porn." These are intimate images that are taken consensually within a romantic relationship and then uploaded without consent on the Internet, often alongside the victim's name, social media information and address. The consequences of this behavior are truly devastating. A person victimized in this way will have these images turn up whenever they are the subject of an Internet search, and because there is no truly reliable way to remove any content uploaded to the internet, the harm can be lifelong. It took months of work to balance the freedom-of-speech concerns with the gravity of the conduct, but I am very confident in our result.

The Privacy Advisor: The Federal Aviation Administration (FAA) recently released proposed regulations for the use of unmanned aircraft systems, more commonly known as drones. The public has debated whether drones represent potentially dangerous invasions of privacy or are positive technological innovations that should not be heavily regulated. Have you heard from Oregon citizens about how they feel about drones and privacy? Do you support the FAA's decision to propose regulations?

Rosenblum: Because Oregon houses several large manufacturers of drone technology, this issue came to us early and we were among the very first state legislatures to craft a legislative response. While I certainly welcome federal guidance on this issue, I also anticipate further work to be done at the state level. Drones can be useful, but like all tools, they can be misused. I look forward to continuing to study drones as part of the much larger continuing

conversation around balancing the incredible potential of these exciting new technologies with the need to defend our privacy as citizens.

The Privacy Advisor: Both data use and data loss issues affect state government and its agencies, just as they do private industry. In many cases, your office advises government agencies on their legal and compliance obligations. How does your role in this respect impact your regulatory and enforcement roles in connection with the privacy obligations of private entities doing business in Oregon or concerning information on Oregonians?

Rosenblum: Under our laws, the rules around protecting personal information apply equally to state agencies and to industry. My office has protocols in place to deal with situations of this nature.

Author Biographies

Divonne Smoyer, CIPP/US is a partner at the law firm Reed Smith LLP in Washington, DC, where she specializes in legal and policy matters involving state attorneys general and consumer protection, including in the areas of cyber security and data privacy. She has extensive experience counseling major corporations through government investigations and litigation, as well as private litigation and in connection with legal and regulatory issues. She frequently writes and speaks on privacy issues and reforms, and is a member of IAPP's Education Advisory Board. Smoyer is a CIPP/US and a graduate of Smith College, summa cum laude, and Harvard Law School, cum laude.

Christine Czuprynski focuses her practice specifically in the area of data privacy and security, as well as telecommunications and marketing, as part of the firm's Information Technology, Privacy & Data Security Group. Prior to joining Reed Smith, Christine was an Assistant Attorney General in the Consumer Fraud Bureau of the Illinois Attorney General's office.