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

Q&A with Massachusetts AG Maura Healey


Divonne Smoyer, CIPP/US


Kimberly Chow, CIPP/US

Massachusetts Attorney General Maura Healey

Attorney General Maura Healey of Massachusetts has held her office since January 2015. Massachusetts has established itself as being on the cutting edge of data privacy regulations that call for robust written information security program and computer system requirements, and the attorney general's office continues to be on the forefront of enforcement since its security breach notification law was passed in 2007. Healey was no stranger to the work of the office, having also served as chief of the Public Protection & Advocacy Bureau and chief of the Business and Labor Bureau, in addition to working as a special assistant district attorney and in private practice. Healey talks to The Privacy Advisor about her work in targeting healthcare-related privacy violations as well as the future of enforcement in our data-driven economy.

The Privacy Advisor: Protecting consumer privacy has been a cornerstone of activities of the Office of the Massachusetts Attorney General, particularly with respect to protected health information. In 2015, you began investigating the Anthem data breach, which affected almost one million Massachusetts residents. There has been a recent rise in other HIPAA-covered entities being targeted by hackers, as well, and your office has investigated data breaches at a number of Massachusetts-based hospitals. What are the implications of this growing area of cybersecurity vulnerability?

AG Healey: The healthcare industry's increased reliance on technology makes it more important than ever that physicians and health providers ensure patients' personal information and protected health information is secure. To prevent breaches like the one at Anthem – which affected the personal information, including Social Security numbers, of millions of its customers and employees nationwide – companies, hospitals and other health care practices must put in place and enforce reasonable administrative, technical and physical security measures. It is their responsibility to understand and comply with our state's data security laws and federal data privacy requirements under HIPAA and the HITECH Act, and to take the necessary actions to ensure that all affected patients are informed of potential harms.

Identity theft is a serious crime with serious costs for victims who may lose significant money and time, and may find their reputation, health insurance and credit rating damaged. Identity theft that leads to compromised health information can have even more serious implications. Our office takes reports of data breaches very seriously and wants to be sure that consumers know how to protect themselves.

The Privacy Advisor: In the same vein, at the IAPP Global Privacy Summit this April, several attorneys general indicated that states are looking to shift their attention from retail breaches, which typically involve credit card information, to breaches of "higher-risk" personal information, including health care data. Do you agree with that statement, and what can we expect from Massachusetts?

AG Healey: Our office examines all data breach notifications that are sent to us, whether those breaches affect credit card information or medical information. It is true that medical information is typically worth more on the black market than credit card information, and that when an individual's medical information is compromised there can be dire consequences for the consumer. We

have seen the payment card industry has reformed in response to the prevalence of merchant breaches involving compromised credit card data to include additional protections for consumers as part of their standard business practice, but more can be done. Although breaches of medical information and other "higher risk" data such as Social Security numbers receive particular scrutiny by this office, we will continue to devote resources to certain credit card breaches that may indicate larger problems with a company's overall data security program.

The Privacy Advisor: Last year, your office testified in front of Congress against a bill that would have established nationwide data breach notification standards because it threatened to weaken the strong consumer protections provided by Massachusetts law. Other attorneys general have recently advocated for the harmonization of state data breach laws due to the difficulty for national companies who are aiming to comply with the many different requirements. Do you believe that such a harmonization is feasible in a way that would protect Massachusetts residents?

AG Healey: Massachusetts has some of the most robust data breach notification and security laws in the nation. The Data Security and Breach Notification Act of 2015 as proposed would drastically undercut existing regulations that provide meaningful consumer protections for our residents. Last July, I led a bipartisan multistate effort to maintain our strong state consumer protection laws, urging the U.S. Congress that any future federal data breach and security law allows states to enforce their own laws and enact new ones to address future data security risks. We should not be preempting state laws, including Massachusetts' stringent data security regulations – regarded as a benchmark nationwide – to establish a vague national standard that leaves consumers without recourse or protection. Residents across this country need strong protections against data breaches and identity theft, so we must work together to ensure that federal law does not leave consumers vulnerable.

That being said, we understand the challenges a company faces in the wake of a breach to adhere to nuanced variations in state breach notification requirements across the country. A unified federal notification standard should allow for states to continue to receive the breach notices that enable our enforcement efforts on behalf of consumers across the country.

The Privacy Advisor: Your office recently hosted a forum on how to protect consumer data privacy while still supporting a data-driven, digital economy. What were your biggest takeaways, and are you optimistic that technological developments will keep consumers' best interests in mind?

AG Healey: We are witnessing in our own backyard the growth of an exciting, forward-looking industry fueled by consumer data. Data-driven technologies are expanding access to opportunities for economic and social advancement. My office supports the growth of a data-driven digital economy, but as we expand what's possible, it's our job to guard against abuse, to make sure that data-driven innovations are a benefit for everyone, including the most vulnerable.

This forum opened a dialogue with consumer advocates, privacy experts, industry leaders and technology innovators to discuss the risks of consumer privacy, and the role of states and state attorneys general in addressing those risks without restricting innovation and advances that benefit consumers in Massachusetts. My office is focused on that balance. We need to lead a data-driven, digital economy that has the potential to expand social and economic opportunities for everyone. But we need to be aware of the risks involved. This forum was about encouraging innovation while ensuring that all consumers are treated fairly in the process.

The Privacy Advisor: You have expressed concern over practices that encourage the collection and sale of inaccurate data about consumers on the open market, and to that end, you led a multi-state filing in the U.S. Supreme Court case Spokeo v. Robins, encouraging the court to recognize how those practices harm consumers. What do you think are the implications of the court's decision for similarly situated consumers in the future?

AG Healey: I have serious concern over practices that encourage the collection and sale of inaccurate data about consumers on the open market, which can cause Massachusetts residents to lose out on access to credit, housing, insurance, and employment opportunities. Big data and data analytics have the potential to perpetuate and facilitate illegal discrimination – such as marketing campaigns that rely on data reflecting race or socio-economic status to promote predatory lending and insurance products, or to steer vulnerable consumers towards illegal or unfair financial products and into a spiral of debt.

In Spokeo v. Robins, I urged the U.S. Supreme Court to recognize the harms that consumers suffer when inaccurate information about them is disseminated and relied upon by businesses. False personal information can cause negative consequences to consumers who are often unaware when their data is circulated, how it is used, or by whom. Consumers must have the ability to redress these injuries. We will be following further developments in the Ninth Circuit in the Spokeo case as well as other lower courts' application and interpretation of Spokeo.

The Privacy Advisor: Given the large number of educational institutions in Massachusetts, how has your office addressed the privacy of students?

AG Healey: Identity theft among our student population is a huge concern. Stealing someone's personal information — such as your Social Security Number, credit card or account numbers, passwords, among others — can impact the ability to obtain loans for education or housing, or damage a student's credit, affecting approval for rental agreements, credit cards or large purchases requiring credit.

Keeping vigilant is the best defense against these fraudulent practices. Our Community Engagement Division has held Community Action Hours relating to identity theft prevention and other consumers issues all across the state, bringing our resources directly into communities at times that are convenient for people. We want to be a source of education and assistance for consumers, including parents and students, on how to prevent identity theft, including steps they can take to recover if they become a victim. For more information we encourage people to visit our website.

The Privacy Advisor: Your office has been involved in several multi-state privacy investigations, including the investigation of Target following its breach of customer information in 2014. What are the benefits of multi-state investigations in the privacy context, and how should businesses respond to multi-state investigations?

AG Healey: With large-scale consumer data breaches like Target, our office works with attorneys general across the country to determine whether the company had proper safeguards in place to protect personal information. Our office has led multiple investigations into potential violations of the state's data protection laws, resulting in significant consumer settlements ensure that these kinds of breaches do not happen again.

As a result of investigations and enforcement actions brought to address a select number of these breaches, our office has developed an expert view into the nature, extent, and frequency of data breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

***Divonne Smoyer**, CIPP/US is a partner at the 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 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.*

***Kimberly Chow** is an associate in the Information Technology, Privacy & Data Security and IP, Information & Innovation groups. She is an IAPP (International Association of Privacy Professionals) Certified Information Privacy Professional (CIPP/US). With a background in journalism and as a former legal fellow at the Reporters Committee for Freedom of the Press, Kimberly brings her experience with the First Amendment and other free speech issues to her privacy and data security practice.*