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

Q&A: DC Attorney General Karl Racine talks consumer privacy

Divonne Smoyer, CIPP/US

Kimberly Chow, CIPP/US

The Privacy Advisor | Apr 26, 2016

District of Columbia Attorney General Karl Racine

Attorney General Karl Racine is the District of Columbia's first elected AG, a position in which he has served since January 2015. General Racine has a deep background in both public service and the private practice of law. As AG, he has quickly earned a reputation as a thought leader among his fellow AGs in a number of important areas, including in the areas of government and consumer privacy. General Racine talks to The Privacy Advisor about his work in the area of consumer privacy for the citizens of the District of Columbia as well as privacy concerning government agencies.

The Privacy Advisor: When you took office, you pledged to make consumer protection a priority. How does data privacy figure in your consumer protection plans?

AG Racine: Data-security laws and breach-notification laws contain important protections for consumers. Our office is working on ensuring these laws protect consumers in two important ways. First, we are reviewing the District's data-breach law to ensure it adequately protects consumers. Second, we – like many other state and federal agencies – are involved in investigating particular data breaches. Where such investigations show that responsible persons failed to take reasonable steps to protect the data they collected from consumers, we will take appropriate enforcement actions. We are also concerned that persons who collect consumers' data do so in an open and transparent fashion and do not mislead the consumers who trust them with their data.

Our office is also relatively new in that we became an independent agency, led by an elected Attorney General, at the beginning of 2015 after previously being subordinate to the District's Executive Branch. Given the new nature of our office, we have greatly expanded our community-outreach efforts, including by expanding consumer education. One of the most important areas of consumer education is teaching consumers how best to protect their data, and, when their data is lost or stolen, how to protect themselves. We are actively seeking to educate consumers through multiple channels, including community meetings, consumer-education materials, social media and traditional news media.

The Privacy Advisor: You signed a National Association of Attorneys General (NAAG) letter to Congress last July, joining 46 other attorneys general in arguing against a federal breach notification and data security law that would preempt state standards. Recently, California Attorney General Kamala Harris called for a harmonization of state data-breach laws that would ease compliance burdens while retaining standards that protect consumers. What advice do you have for businesses who must comply with the myriad state laws, and what are your views on harmonization of the laws without a federal standard with preemption?

AG Racine: Most state data-security laws boil down to two very important concepts. First, persons who collect consumers' personal data need to tell consumers when they are collecting their data, if they share such data, and other relevant information concerning their privacy practices. Of course, persons must then comply with their stated practices. This can be accomplished with a well-thought-out privacy policy and privacy notice. Second, persons must take reasonable care when collecting and maintaining consumers' personal data.

With regard to data-breach laws, I support a harmonized federal standard, provided state attorneys general are not preempted from taking actions against parties that violate our own state (or in my case, District of Columbia) laws designed to protect consumers' data.

The Privacy Advisor: This past November, you joined eight other AGs in a letter to credit card companies, urging them to expedite the implementation of chip-and-pin technology, which you stated would better protect consumers from breaches of their personal financial information. What do you see as the role of AGs in advocating for certain technologies?

AG Racine: Our office joined this letter because credit- and debit-card safety is a vital area of consumer protection – and chip-and-pin technology has a strong track record in reducing consumers' exposure to card fraud in places where the technology is used. France, Canada and the U.K. have reported significant reductions in multiple kinds of card fraud since they adopted chip-and-PIN technology. While it's good that our country is now moving from magnetic-strip technology to chip-and-signature technology, the safest bet is to move to the even stronger chip-and-PIN technology. The problem in our country is huge: Since 2003, the U.S. has consistently accounted for about half of the global loss from fraudulent transactions, despite being responsible for only a quarter of total card payments.

The Privacy Advisor: Your office also counsels (and defends) government agencies on privacy protections, data use and data loss. Government agencies at all levels are not immune to data losses, data misuse and hackings. How do your roles in these areas impact your approach to privacy enforcement vis-à-vis the private sector?

AG Racine: Attorneys general are charged with enforcing state UDAP laws and Data Security Laws, notwithstanding the potential or realized data breaches experienced by other government agencies. As the District's chief law enforcement officer on consumer issues, including privacy, I am concerned about public institutions maintaining good data collection and maintenance practices as private ones. Just like our residents deserve to have their data protected, every customer of every business deserves to have her data protected.

The Privacy Advisor: Washington, DC, is unique in that has is its own government (albeit that it is not a state), yet by virtue of its location of the federal government, it is at the epicenter of national and international discussions on policy (including an apparent disagreement between the U.S. Department of Justice and the Federal Trade Commission on requirements that companies provide for so-called "backdoor encryption" keys for use in law enforcement situations), including policy on data privacy. How does this affect how you run your office, advise DC agencies and pursue enforcement actions?

AG Racine: This Office is placed no differently than other state attorneys general in that we look to the decision-making of other federal agencies in the area of privacy; particularly the FTC's interpretation of Section 5 of the FTC Act. We are not, however, bound by such decision-making. One informal way in which our office's thinking about data privacy is impacted by our unique location is the access we have to individuals and organizations with extensive knowledge of the national and international landscape in the data-privacy space. Simply by virtue of living in the same metropolitan area, attorneys and staff in our office regularly encounter data privacy experts in the federal government, as well as the private and non-profit sectors. This interaction helps us stay abreast of trends, developments, and best practices in a way that, I think, ultimately redounds to the benefit of our consumers.

***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.*