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

Mississippi AG: Best To Notify Us Quickly of A Breach

Divonne Smoyer, CIPP/US

June 18, 2015

Mississippi Attorney General Jim Hood

Mississippi Attorney General (AG) Jim Hood is the president of the National Association of Attorneys General (NAAG), the professional association for the AGs of all 50 states, DC and the U.S. territories. As NAAG president, Hood has selected cybersecurity and digital privacy, as well as counterfeiting and IP theft, as topics of policy focus for NAAG. He also recently presided over NAAG's National Presidential Initiative Conference, "Protecting Our Digital Lives: New Challenges for Attorneys General," in Biloxi last April, which brought together more than a dozen AGs and their staffs to focus on these issues. In this spotlight, Hood discusses his NAAG presidential initiative, his interest in cybersecurity and digital privacy and what we can expect to come from his work in these areas.

The Privacy Advisor: For the past year as NAAG president, you have been at the forefront of encouraging your fellow AGs to educate themselves and their staffs and flex their muscles as regulators concerning evolving issues of data privacy and cybersecurity. Why these issues; why now, and why should AGs make these priorities?

Hood: Although data privacy and cybersecurity are the focus of my work as NAAG president this year, my fellow attorneys general and I have prioritized these issues for at least a decade. AGs fight each day to prevent and address identity theft, have passed security breach notification laws in almost every state and routinely take other steps to ensure the safety of our states' citizens in the Digital Age. Over the past decade or so, AGs have seen rapid advancements in these areas. For example, our office has had a steady increase in the number of identity theft reports, and the instances of potential data breaches has increased significantly. As AGs, we work together to address nationwide security breaches when they occur, and we try to educate businesses and other organizations on prevention.

Another growing concern that has worsened in recent years is online intellectual property theft. As AG, I've fought hard to protect consumers from fake goods, especially those that can harm or even kill consumers like pharmaceuticals, auto parts and similar items. Just last month, I hosted an initiative on these very issues. We focused on collaboration in the area of cybercrime, particularly in the area of counterfeit goods being sold in the virtual world. These online operations are widespread and sophisticated, so pooling our resources at the state and federal level is critical. That's what we have done in Mississippi with the formation of an intellectual property theft task force made up of local, state and federal officials. We've been very successful in catching perpetrators who are trying to sell fake, and often unsafe, goods to Mississippians.

Another area of focus for our office has been education. This includes education of consumers in the areas of identity theft, counterfeit goods and other crimes that often occur online. It also includes training of fellow law enforcement agencies on how to spot and address these issues. Most AGs approach these issues like we have: using education to encourage prevention but being prepared to address at a civil or criminal level when an incident occurs.

The Privacy Advisor: The topics of your NAAG presidential initiative reflect ongoing debates at the national level about not only how private entities use personal information but also how such information is used by the government and, in particular, law enforcement. In a number of instances, the FBI, the Secret Service and state and local prosecutors have stressed to AGs at NAAG meetings within the past year that they need access to digital information, particularly information on cell phones, to perform investigations and solve crimes. Is there consensus among AGs about how best to balance the privacy of individuals along with the need by law enforcement for information to help solve crimes?

Hood: That's a good question, and the answer is complicated. I know all AGs want to make sure that consumer privacy is respected in accordance with constitutional principles. As law enforcement officials sworn to uphold the laws, we also want to pursue all legal avenues for collecting critical evidence that can be used to solve crimes and, in turn, protect our citizens. As we investigate in real time, we have to be able to seek and use evidence available to us to bring criminals to justice. This could mean using information on cell phones—which everyone uses now like computers—to investigate.

But the balance comes in the way we obtain that information, such as when a warrant goes through the judicial branch and allows an independent assessment of the request, or when an appropriate exception to the warrant requirement exists. The bottom line is that although the technology has changed, the avenues for appropriately seeking evidence have not. The legal and evidentiary borders simply have to be evaluated in light of emerging technology and privacy concerns. We'll leave it to the courts to set the appropriate balance.

The Privacy Advisor: And, speaking of government use of data, it is no secret that state agencies themselves have been the subject of hackings and other security breaches, just as private entities have been. In fact, a recent NAAG report lists nearly two dozen state agencies—in Alabama, California, Connecticut, Florida, Iowa, Illinois, Maryland, Michigan, North Carolina, New Jersey, Oregon, South Carolina, Virginia, Washington and Wyoming—that experienced breaches in the first three quarters of 2014 alone. While a major job of an AG is to protect state consumers from data loss or inappropriate data use by private entities, his or her job also is to advise and defend state agencies in these same areas. How are you and your fellow AGs juggling those roles?

Hood: Attorneys general are often called upon to play dual roles, and the area of security breaches is no different. If a state agency is the subject of a hacking or a security breach, AGs must ensure that the agency complies with all applicable state laws. This could mean providing notice to affected individuals, investigating the source of the breach and taking other remedial action. On the other hand, our job as AGs is to protect the very consumers affected by the breach. This dual role—while it may seem contradictory—is not really a juggling act. Instead, AGs are typically given the constitutional or statutory duty to serve both roles, provided separate attorneys in our office handle each "side" of the issue. The AGs' deep understanding of these issues from all angles helps the agency and the affected individuals.

The Privacy Advisor: It has been said that technology has been changing so rapidly that as soon as a law or regulation governing its use is put in place, it is already out of date. Are there particular areas where you have found that to be true in your work, or are existing state or federal frameworks capable of adequately regulating these new technologies? For example, do existing laws protecting Mississippians from unfairness, fraud and deception suffice in the privacy and cybersecurity contexts?

Hood: I think the biggest challenge facing legislators and other rule-making bodies is the ability to apply a law that adequately covers the offense to a particular scenario. We have strong laws prohibiting cybercrime, identity theft and fraud. Sometimes it's not the substance of the offense or statute that needs to change but the definition. We frequently use our cybercrime, consumer protection and identity theft laws to prosecute offenders. As a result, we sometimes have to argue that a definition includes a certain set of facts. In other words, we may have to change some definitions to make the laws more inclusive but not the statute authorizing action. It's a fine distinction, but it sometimes makes necessary changes easier.

The Privacy Advisor: Like most states, Mississippi has a data breach notification law that requires breached entities to notify Mississippi residents who may be affected by a breach of security. For the last decade, Congress has considered federal breach notification proposals that have failed to gain traction. This spring, there appears to be some glimmer that such legislation may actually pass. Bills that are getting the bulk of the attention purport to preempt state data breach notice laws but allow AGs to enforce a federal breach notice law. Do you have an opinion on such a law?

Hood: To ensure that all citizens are being protected from data breaches, particularly those in states where no notification law exists, I believe we need a dual federal-state role in enforcement. A federal data breach law should not replace or preempt state law. Instead, it should provide an additional layer of protection for consumers. Countless areas of the law successfully maintain this balance between state and federal enforcement, and it ensures all breaches—no matter how large or small—can be addressed. If a bill providing for preemption passes, I think most (if not all) AGs would want the ability to enforce the federal law. This has worked well for specific privacy laws, like HIPAA.

As I mentioned, education is key in the area of data breaches. We have working groups through NAAG that address widespread security breaches, but those groups also discuss ways we can "get ahead" of the problem by urging businesses to take steps to prevent security breaches. I know that the Department of Justice recently released "Best Practices for Victim Response and Reporting of Cyber Incidents," a booklet of helpful tips on preventing and addressing cyber intrusions. In addition, as part of my presidential initiative to address the challenges of cybercrime, Mississippi is working with other states to further develop cybersecurity suggestions to educate small to medium businesses and other entities and to provide a list of existing resources and standards. Failure to be proactive in updating policies and training employees is dangerous for any size business. Although AGs understand the resources required to analyze and implement changes, the price of failing to train and update could be far greater. The upside of investing in updating policies is that under our statute, a company that has a security breach policy could automatically satisfy the Mississippi security breach requirements—and this would be in true in some other states as well.

Despite these prevention efforts, breaches will occur. I think most AGs would agree with me that a common misperception is that businesses should not contact us when a breach is discovered. But chances are, we will hear about the breach, so it's best to notify AGs quickly. Although it is true that notifying AGs in affected states will not preclude an enforcement action, it could lessen any penalties resulting from the company's failure to safeguard information or notify consumers.

As AGs, our ultimate goal—and duty—is to ensure that proper notification and remediation occurs following a breach. If businesses and other organizations possessing sensitive information take steps to prevent breaches, and we have strong breach notification laws—state or federal—consumer data will be safer in the long run.

***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.*