Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ashley Madison Action Shows Global Regs Can't Be Cheated

By **Allison Grande**

Law360, New York (August 26, 2016, 5:08 PM ET) -- Canadian and Australian data protection regulators recently came down hard on infidelity site Ashley Madison for having inadequate security safeguards in place at the time of a hack that exposed 37 million members' data, demonstrating the growing willingness of regulators outside the U.S. and European Union to bring down the hammer on companies that ignore data security risks.

Since Ashley Madison, which is owned by Avid Life Media, revealed last July that hackers had obtained and publicly released profile information and email addresses of about 37 million users, the company has faced intense backlash, including hundreds of lawsuits lodged by irate members and a probe that has reportedly been initiated by the Federal Trade Commission.

The fallout continued Tuesday, with the privacy commissioners of Canada and Australia releasing a report that was notable not only for its conclusion that Avid Life Media had far from adequate information security procedures in place at the time of the hack, but also for its authors.

"The internet doesn't know geographic boundaries, and websites that reach outside the U.S. need to know that they can face enforcement actions by the regulatory authorities of other countries," Duane Morris LLP of counsel Eric Sinrod said. "And because these countries tend to have privacy laws and standards that are greater than those in the U.S., if a company faces potential fallout from an incident in the U.S., it's likely that it's going to face even more scrutiny in some other country."

For companies like Ashley Madison that find themselves at the center of a headline-grabbing data breach, it has become almost a foregone conclusion that they will receive at least questions from the FTC, which has broad authority to probe the strength of corporate data security practices, as well as potential inquiries from regulators such as the Federal Communications Commission and the U.S. Securities and Exchange Commission, which have been ramping up their privacy focus in recent years, but with a more sector-specific focus.

Companies have also been growing somewhat accustomed to hearing from data security authorities in the European Union, which have been more aggressive at pushing companies such as Google Inc. and Facebook Inc. on the legality of their privacy policies and will soon have significantly enhanced powers to levy penalties under an overhaul to the bloc's data protection law set to take effect in 2018.

But while businesses whose operations extend globally are less used to hearing from regulators outside of these two major zones, attorneys say it would be a mistake for companies to ignore these authorities,

which Tuesday's report demonstrates have both the power and the interest to make businesses pay for their security failings.

"The privacy community not just in the U.S. but also in places like Asia and Latin America is becoming much more aggressive about investigating companies that have large breaches and have big global profiles," Nelson Mullins Riley & Scarborough LLP attorney Bess Hinson said. "Hopefully this report highlights the need for companies to be mindful of where their traffic is coming from and, even if it's just a small percentage coming from a certain country, that they need to amend their privacy policy to address that country's unique privacy laws."

The decision by the Office of the Australian Information Commissioner and Office of the Privacy Commissioner of Canada to take a hard look at the Ashley Madison breach is hardly surprising, given the significant fallout reported by its users, including the disintegration of marriages, the loss of jobs, extortion attempts and even the decision by some outed individuals to take their own lives.

"After a hack, the question becomes what the real effect is, and whether it's more of an academic matter or true harm," Sinrod said. "With Ashley Madison, there are so many real ripple effects that it's almost like a case study in privacy, and there are certainly lessons to be drawn for other companies."

The main takeaway for companies centers on a concept that the FTC has longed stressed: Say what you do, and do what you say.

In Ashley Madison's case, the site billed itself as the perfect place to have an affair, a "100 percent discreet" service that assured users that their identities and illicit activities on the site would be kept under wraps. However, the privacy regulators' report found that certain information security safeguards required by both Canada's Personal Information Protection and Electronic Documents Act and Australia's Privacy Act were insufficient or absent.

"Organizations that hold other people’s private personal, financial or medical information need to take their information security and cybersecurity responsibilities seriously," Snell & Wilmer LLP data privacy and data protection group chair Patrick Fowler said. "Failing to immediately address known security weaknesses is a recipe for disaster, both in terms of failing to prevent a breach, and then having to explain why steps were not taken to avoid the breach."

The regulators' report focused on four main issues: information security, retention and deletion of user accounts, accuracy of email addresses and transparency with users.

When it came to information security, the regulators found that Avid Life Media failed to have a comprehensive privacy and security framework, which the report called "a basic organizational security safeguard," and to take precautions such as training its employees and contractors and failing to adequately protect encryption keys and passwords.

In a separate document highlighting takeaways for all organizations, the Canadian privacy commissioner stressed that documentation is essential because it provides "explicit clarity" around privacy and security-related expectations for employees, focuses businesses on the issue, and helps them identify and avoid gaps in their risk mitigation efforts.

"The practical takeaways are, if I collect highly sensitive information about people, I need to make sure I have an 'adequate and coherent governance framework,' and if I am making public statements about

the discretion and security my company maintains to protect that highly sensitive information, then I need to ensure that those statements are accurate," said Al Saikali, co-chair of Shook Hardy & Bacon LLP's data security and privacy group.

The importance of having a comprehensive privacy policy framework in place — and actually following it — is amplified by the increasingly stringent privacy laws that can be found throughout the world.

Many countries, including Canada and Australia, have privacy regimes that come closer to the EU's stringent protections that govern the handling of data than they do to the United States'.

The EU framework was recently revamped to replace the current patchwork regime with a uniform and more stringent general data protection regulation, as was Australia's, which was updated in 2014 to strengthen and unify the country's privacy laws.

The protections surrounding data held in the U.S. are also constantly evolving, with states such as Massachusetts having laws on the books that require companies to have written information security programs that mandate thorough employee training and Florida's data breach notification law giving its attorney general the power to request companies' information security policies in the wake of a breach, attorneys noted.

"It can take companies on the e-commerce side by surprise that they need very specific and comprehensive privacy policy frameworks given today's regulations in the U.S. and abroad," Hinson said.

The regulators' report also offers important reminders when it comes to topics such as data retention and transparency, according to attorneys.

Ashley Madison lost major points for the amount of time it held onto users' data, including those that had explicitly requested — or in some questions, even paid for — their accounts to be closed and their data permanently deleted, which ran directly counter to the requirement in both countries that data only be retained to carry out the purpose for which it was collected.

"Some companies just assume or think it's OK to maintain personal information and store it indefinitely," Hinson said. "But what happens down the road when there's a breach is that the company is potentially exposing information of people who haven't been customers for years, and they're still required to address that exposure."

The regulators also faulted Ashley Madison for failing to verify the validity of customers' email addresses and for putting trust marks on its website that suggested a high level of security, but were later found to be fabricated. Avid Life Media agreed to enter into a compliance agreement with the Canadian Commissioner and an enforceable undertaking with the Australian Commissioner promising to address and fix all of the deficiencies identified by the regulators.

"With all of the attention and resources devoted to encouraging improved cybersecurity over the past few years — particularly since the Target breach in late 2013 — company executives will find it extremely difficult to explain to regulators, customers, shareholders and taxpayers when the security issue is eventually exploited and a data breach occurs," Fowler said. "Ignoring a known security flaw and hoping it will go away is not a reasonable strategy."