DATA PRIVACY AND SECURITY: DON'T FORGET THE BASICS

By **David Gurwin**, Buchanan Ingersoll & Rooney

Much publicity has surrounded a couple of data security and privacy issues over the past six months. First, there was the hack of the Canadian "online cheating" site, AshleyMadison.com, that, due to the nature of the site, led to a feeding frenzy in the media. Then a more significant event occurred: the ruling by the European Union's Court of Justice ("ECJ") that invalidated the "Safe Harbor Agreement" which allowed U.S. companies to transfer European citizens' data to America provided certain conditions were met. The Safe Harbor, which had been relied on by thousands of U.S. companies with transatlantic operations (including e-commerce sites with European customers), previously provided the means by which these American companies could ensure compliance with the very strict EU Data Protection Directive ("Directive"), which governs the protection and transfer of personal data belonging to EU nationals.

Since the ECJ's announcement last October, U.S. and EU authorities have engaged in discussions regarding a new framework to govern transatlantic data transfer, but a mutual solution has yet to be found. Simultaneously, EU authorities are working to develop an entirely new data privacy framework, the EU General Data Protection Regulation, hoping to pass the legislation in early 2016 with full enactment within two years. The new EU legislation undoubtedly will have a large impact on any sort of new transatlantic data-transfer safe-harbor or regulatory scheme, and will also impact companies with European operations in many additional respects.

In addition to the evolution of European data privacy laws, companies should also be mindful of (i) the FTC's Children's Online Privacy Protection Act ("COPPA") to the extent they operate websites or online services directed to children under 13 years of age, or have actual knowledge that they are collecting personal information online from a child under 13 years of age; (ii) the California Shine the Light Law, to the extent they conduct business with any resident of California and have shared customer personal information with other companies for their direct marketing use within the immediately preceding calendar year; (iii) The Financial Services Modernization Act (Gramm-Leach-Bliley Act ("GLB")) to the extent they collect, use or disclose personal financial information; (iv) The Health Insurance Portability and Accountability Act ("HIPAA") to the extent they come into contact with personal medical information; and (v) The Federal Trade Commission Act, a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies, providing for liability to the extent a company fails to comply with its own posted privacy policies.

Though there have not necessarily been any major developments in data privacy law of late (aside from the EU situation discussed above), companies must remember that their business operations, along with data privacy law, can always be evolving, shifting or changing, and as such it is important to engage in a meaningful review of privacy policies with relative frequency, to ensure that the safeguards and protections in place are applicable to the company's then-current state of business operations, and that the company is in compliance with all aspects of its policy and any then-existing applicable privacy laws.

With the notable exceptions listed above, the basic premise for data privacy in the U.S. is rather simple: say what you are going to do (in terms of gathering, using and sharing personally identifiable information) and then do what you said you were going to do. While this is all pretty straightforward, I am constantly amazed at the lack of attention paid to Privacy Policies by otherwise sophisticated companies. Many do not have a stated Privacy Policy (either as part of their website's Terms of Use or as a standalone Privacy Policy). Even those that do have Privacy Policies often forget that these are dynamic documents that need to be updated to reflect the then-current data privacy practices of a company. For example, having an out-of-date policy that states that any personally identifiable information will never be shared when, in fact, the company regularly shares such information with third-party data processors is almost worse than having no stated policy at all.

While most state laws (with a few exceptions, such as Massachusetts) in the data privacy area are focused on providing notice to consumers in the event of a data breach, the Federal Trade Commission ("FTC") has continued to flex its muscles in this arena. Even if there are no specific state requirements in terms of data security standards, the FTC has taken to reviewing whether a company's data security practices have been "reasonable" on an "after-the-fact" basis—often leading to large fines and, often even more damaging, public pronouncements that impact consumers' confidence in the company.

Given all of this, there really is no good excuse not to focus on adopting and updating a Privacy Policy. It is not a complicated process, but the failure to do so could result in significant financial harm and reputational damage to a company.

David A. Gurwin is the Chair of Buchanan Ingersoll & Rooney PC's Technology Transactions Group, as well as its Entertainment & Media Law Group and its Copyright Practice Group. He can be reached at (412) 562-1592 or david.gurwin@bipc.com.