Global Asset Management

Corporations as protectors of privacy

> "There is nothing new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."
>
> – Antonin Scalia, former U.S. Supreme Court Justice

The late Justice Scalia's comments would seem to aptly sum up the very public spat we have seen unfold in the U.S. in recent months between Apple Inc. and the U.S. Federal Bureau of Investigation (FBI). At the heart of it is the ability of government to be able to access private information. This confrontation has posed some fundamental questions about balancing the rights of the individual against the risks to collective security. It also highlights that privacy issues represent a very real and material risk to many companies. It is timely to examine what those risks are and the impact privacy, or a lack thereof, can have on corporations and the products and services they sell.

Is there a right to privacy?

The "right" to privacy is something that varies greatly depending on where you live. The U.S., for example, takes a different approach to privacy than most other developed countries. The U.S. Constitution does not contain any express right to privacy although it does allude to certain aspects of privacy, for example, by preventing unreasonable search and seizure. When it comes to information privacy, the U.S. is notable for not having enacted a comprehensive information privacy law. What it has done is enact various pieces of legislation that address information privacy in certain sectors and industries. Overall, this means that the protection of private information in the U.S. is not as robust as in other developed countries.

A good example of robust protection of private information can be found in Europe. European governments collectively recognized the right to privacy by specifically including the right in the European Convention on Human Rights, which was adopted in 1950. The European Union (EU) harmonized protection of personal information across member states by adopting the Data Protection Directive in 1995, and all member states plus Switzerland have enacted legislation to comply with the EU directive.

Canada has its own privacy legislation, which is also compliant with the EU directive. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into force on January 1, 2001. Since then, most provinces have also adopted complementary legislation. PIPEDA clearly defines the rights of the individual and the obligations of the organizations that collect personal information. This includes obtaining consent before information is collected, used, or disclosed. It also includes an obligation to safeguard the information that is collected.

This obligation that requires companies to act as stewards of private information and protectors of privacy has created certain risks for these companies. When companies fail in these obligations there can be very real implications in terms of brand and financial loss. For investors, privacy risk has become investment risk. This has been demonstrated in some recent cases.

A bad apple

The recent case of Apple Inc. vs. the FBI in the U.S. has demonstrated just how important privacy issues can be. Apple was asked by the FBI to help access the iPhone used by the mass shooter in San Bernardino, California in December 2015. The iPhone encryption, password, and the self wipe feature presented an obstacle the FBI could not overcome without the help of Apple. Apple has cooperated with the police and security services on many cases in the past, but this time it was different. The FBI was not just asking for help, they were asking for Apple to build a back door to the iPhone. Apple was uncomfortable doing this because it was not just facilitating access to this one phone, but potentially to all iPhones, and to anyone who could obtain the technology if it got beyond just Apple and the FBI. The CEO of Apple, Tim Cook, summed up their concerns when he said that "you can't have a back door that is only for the good guys."

The FBI went to court and obtained a court order for Apple to comply with the FBI request, which Apple was in the process of appealing when the FBI announced that they no longer needed Apple's help as they had gained access to the phone with the help of a third party. Now this debate moves into new and uncertain territory as the FBI has knowledge of a security vulnerability that, in theory, weakens Apple devices around the world.

Apple is not the only phone maker to be faced with this issue. In late 2015, BlackBerry was facing demands from the Pakistan Government for access to BlackBerry user data, including emails and BBM messages. BlackBerry decided that they would prefer to exit the Pakistan market rather than allow this type of access. In the end, the Pakistan Government backed down and BlackBerry will continue to operate in Pakistan.

Both the Apple and BlackBerry cases highlight that technology companies are very reluctant to compromise on privacy issues. Technology companies, Apple included, are even taking steps to lock themselves out of their own customers' devices, deliberately making it harder to fulfil official requests for access. While these companies likely see this as the right thing to do, perhaps the greatest motivator for these actions is that they recognize the importance of their commitment to privacy, product success and brand value. Compromise this commitment to privacy and this could, in turn, affect confidence in the product. This could lead to lower sales and reduced revenue, in turn, directly impacting performance of the stock. This direct link between privacy and stock price is why investors should be aware of the potential implications of what the Apple vs. FBI case represents.

Once more into the breach

The other aspect of privacy risk that companies must manage is the private and confidential information that is provided by customers and retained by the company. This could be anything from a name and address to credit card details and information about health and lifestyle. As mentioned above, companies have an obligation to protect the private information that they collect, but unfortunately it is becoming more and more common for that information to be breached either by the company inadvertently disclosing the information or, more commonly, by hackers breaching the company's systems. This is of great concern to all of us as individuals because of the threat of things such as identity theft, but this is also a concern for companies as a breach of confidential information can damage the brand and sales, and result in significant direct costs.

A recent example of how material a breach can be to a company's fortunes is the retailer Target. In December 2013, in the midst of the busy Christmas season, Target discovered that their systems had been breached and that the details of approximately 40 million credit and debit cards had been compromised. The impact on the company was immediate and continues to be felt more than two years later. The company spent $61 million in the first two months to cover damages of the breach, and sales were 46% below that of the same period the previous year. Target settled a claim with Visa in the amount of $67 million to partially compensate them for the cost of reissuing cards, and will likely settle for a similar amount with MasterCard. There are also a number of other claims outstanding from other card issuers.

While it is relatively easy to determine what the direct costs to a company are for a breach, what is harder to quantify is the impact on the reputation and brand of a company. This is often determined by how the company manages the breach and how proactive they are with addressing the concerns of their customers. A 2015 survey[1] found that the event that had the greatest impact on brand reputation was a data breach, followed by poor customer service and environmental disaster. For a company like Target in the highly competitive retail sector, a data breach of private information could be disastrous. However, Target is not alone. Companies such as Home Depot, Sony, Sears, JPMorgan Chase and many more have suffered similar breaches. So many, in fact, that security experts now consider there are two types of companies; those that know they have been breached and those that don't know they have been breached. There is some evidence to suggest that the impact of a breach on a company's stock price is becoming less pronounced as breaches become more common. It appears that both the general public and shareholders are becoming numb to the news of yet another breach, and that privacy breaches are becoming less of an "event" and more just an ongoing cost of doing business.

Beyond the regulatory requirements and the national security considerations, a commitment to the protection of privacy has become an important element of the brand and reputation of all companies. Once the trust around privacy is lost, it can be difficult and expensive to get it back. Importantly, for investors, this can directly impact how these companies perform.

[1] The Aftermath of a Mega Data Breach: Consumer Sentiment. Survey conducted by The Ponemon Institute and sponsored by Experian's Data Breach Resolution Unit.

Publication date: April 15, 2016. IC1611600

Global Asset Management

(05/2016)
016GAM031_(05-2016)_CORP_PROTECTORS_EN_V1_2_FNL 05/26/2016