REPRINT FINANCIER WORLDWIDE

JUNE 2018

FINANCIER WORLDWIDE corporatefinanceintelligence

RISK MANAGEMENT

Data privacy and cyber security: the importance of a proactive approach

MARTIN M. ZOLTICK AND JENNIFER B. MAISEL

ROTHWELL, FIGG, ERNST & MANBECK, P.C.

New laws are taking effect across the globe to regulate the collection, use, retention, disclosure and disposal of personal information. At the same time, the rate of cyber attacks, data breaches and unauthorised use of personal data is growing exponentially. In the current environment, it is more important than ever, particularly for those organisations handling financial data, health information and other personally identifiable information, to understand the rights and obligations of individuals and organisations with respect to personal information.

This article provides an overview of some of the new data privacy laws, rules and regulations that are, or soon will be, in effect, outlines cyber security and data protection best practices and compliance programmes to help organisations comply with the evolving new data privacy requirements, and touches on the role of new technologies in mitigating risks and supporting compliance.

ROTHWELL FIGG
IP Professionals

Martin M. Zoltick is a member and Jennifer B. Maisel is an associate at Rothwell, Figg, Ernst & Manbeck, P.C. Mr Zoltick can be contacted on +1 (202) 783 6040 or by email: mzoltick@rfem.com. Ms Maisel can be contacted on +1 (202) 783 6040 or by email: jmaisel@rfem.com.

ROTHWELL FIGG
IP Professionals

The emerging data privacy regulatory space

The European Union's enforcement of the Global Data Protection Regulation (GDPR) commences on 25 May 2018, and with it comes sweeping changes in the privacy and data security policies for the vast majority of companies operating, not only in the EU, but across the globe. This is because the GDPR applies to all companies processing the personal data of subjects residing in the EU, regardless of the company's location, and generally governs how companies manage and share such data.

Provisions of the GDPR that will be important for all companies to take note of include the requirement for explicit and informed consent for collecting personal data and mechanisms to withdraw such consent, breach notifications, the right to access all data that a company has collected, and the right to be forgotten through the erasure and cessation of the dissemination of data. Penalties for breach of the GDPR are steep – up to 4 percent of annual global turnover or €20m, whichever is greater.

The regulatory environment in the US comprises a somewhat convoluted, patchwork system of federal and state laws governing privacy and data security concerns that is continuing to evolve to try to address the rash of data breaches and unauthorised use of personal data that are occurring with ever-increasing frequency. All 50 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands have enacted laws requiring notification of security breaches involving personal information. Companies may face both civil and criminal penalties for a data breach of sensitive information, and some state and federal laws provide the right for individual citizens to file class action lawsuits for privacy violations. Massive class action lawsuits, like the 2013 Target data breach litigation and the currently pending 2017 Equifax data breach litigation, highlight the significant risks that companies face in the wake of a cyber security attack or as a consequence of either not having best practices and compliance programmes in place or simply not following them.

Importance of cyber security and data protection best practices and compliance programmes

The stakes have never been greater than they are right now with respect to the collection, use, retention, disclosure and disposal of personal information. With the present regulatory framework and knowledge of where it is heading, companies can expect to continue to face rising costs and escalating risks associated with their privacy and data security practices.

A number of resources are available that can provide guidance and assistance with addressing privacy and data security practices, as well as to ensure that the practices and programmes implemented are compliant with relevant laws and regulations. The EU and some US Federal agencies, including the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST), have been promulgating updated guidelines and recommendations for privacy and data security best practices in a variety of industries, including some of the newer Internet of Things and peer platform (sharing economy) marketplaces. Additionally, several industry groups have adopted self-regulatory programmes and rules, including certification programmes, to which a company can voluntarily abide.

ROTHWELL FIGG
IP Professionals

In view of these guidelines and others, companies are further encouraged to establish internal policies and procedures to ensure compliance. Business policies may include a top-level information security and privacy policy, which expresses a commitment to data security and privacy from the top-level officers of a company, a risk management programme, an acceptable use policy, access compartmentalisation, communications monitoring, breach reporting, a document retention policy and outsourcing policies. Technical policies may include a variety of commitments to technical controls to ensure the protection of data, including encryption, passwords, authentication protocols, disaster recover, intrusion detection, physical security, patching and the like.

For companies with a public-facing website, website privacy policies are a must. Additionally, a written incident response plan is critical for establishing protocols for initiating a response team, assessing data breach activity, containing the data breach, and providing guidelines for including other parties, such as law enforcement and officials that require notification under data breach laws. Further, a company must continue to audit and maintain certification as necessary to ensure that their policies and procedures are enforced and remain current. A variety of enterprise privacy management software and compliance solutions may be used internally to help companies audit their systems.

Privacy and data security must be part of the conversation when utilising new technology

While it may be easier said than done to implement new policies and best practices, companies are faced with the additional challenges of evaluating and deploying new technologies that simultaneously may both hinder and help with compliance in view of the new privacy and data security regulations. For example, blockchain technology offers significant advantages for a wide variety of applications from a data security perspective, offering the ability to record transactions in a decentralised and immutable fashion. However, these same technological principles may raise complex issues when looking at compliance with new privacy regulations. For example, in connection with the "right to be forgotten" under the GDPR, how is a subject's personal information to be erased from an immutable and fully-distributed blockchain? A variety of solutions have been proposed to provide for greater control and management of information with blockchain, including anonymous transactions and voting systems, secret contracts and blind auctions, but they will have to be evaluated in view of the evolving regulatory framework.

Artificial intelligence (AI), and specifically machine learning (ML) techniques, are now widely employed to enable computers to learn and adapt to new input. Such AI technology can be used in cyber security systems to provide automated processes for the identification of new threats and the implementation of technology controls and protection. On the flipside, hackers have also started to weaponise AI, creating programmes that can study systems, evaluate vulnerabilities or even create persuasive phishing schemes based on the behaviour of social networks. AI applications may also raise privacy issues, especially given the large volume of data required to build a model and the often 'black box' lack of transparency behind the logic used

ROTHWELL FIGG
IP Professionals

by AI agents to arrive at a decision about a person.

New outward-facing tools and platforms have also been developed in order to allow users to control how their data is being used. For example, Facebook recently released a set of privacy tools, including a unified privacy dashboard, and has announced the launch of a new clear history tool. Such tools cannot be overlooked, as they may be essential for compliance with the new privacy regulations, such as data portability, right to be forgotten, and withdrawal of consent of the collection of personal data.

Conclusion

Recognition of the new and evolving international privacy and security regulations is a requirement, especially in view of the threat of increasing liability and risk with statutory penalties and class action lawsuits. Implementing a compliance programme with a set of best practices for privacy and data security will surely help mitigate these risks, but it is a continuing process, especially as companies face new hurdles when rolling out new systems and technologies.

This is particularly true where newer technologies, such as blockchain and AI, are incorporated into systems in a manner that simultaneously offers important contributions to security and privacy while exposing new vulnerabilities and concerns. Thus, companies may be well-served by a privacy by design approach that promotes privacy and data security compliance from the start in order to mitigate risk down the road. ■