Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cyber Security

USA
McGuireWoods LLP

chambersandpartners.com

2019

Trends and Developments

Contributed by McGuireWoods LLP

McGuireWoods LLP attorneys come from all practice areas impacted by cybersecurity and data privacy: regulatory, litigation, corporate, supply chain, intellectual property, employment, technology, outsourcing, and insurance. Our team also focuses in specific industries with significant privacy concerns such as financial services, healthcare, energy, and retail. Our strong EU/cross-border practice includes lawyers in London and Brussels. Lawyers assist clients with information assurance, information governance, incident response and remediation and cutting-edge technology issues.

Authors

Steve Gold has 30 years of experience as a technology lawyer, including technology transactions, blockchain technology, Internet of Things, and authentication. He is a partner and chair of the technology and outsourcing practice. He is a member of Sections of Business Law, and Science & Technology, Cyberspace Law Committee, American Bar Association, Association of Computing Machinery, The International Technology Law Association. He has authored a number of industry publications.

Janet Peyton has over 20 years practising intellectual property law and more than 15 in the areas of preventive data security and managing compliance issues in the aftermath of a data breach. She is a partner and chair of the transactional intellectual property practice. Her experience includes auditing and evaluating clients' data security policies, drafting website privacy disclosures and internal corporate privacy policies, negotiating cloud computing agreements from both the vendor and customer perspective, and compliance with breach notification laws. She holds CIPP/US certification as a Certified Information Privacy Professional from the International Association of Privacy Professionals (IAPP). She writes regularly for industry publications.

Biometrics

Unique physical characteristics are increasingly being used as a means to authenticate access to systems and data. The use of biometrics in smartphones has helped bring this technology into mainstream culture. Not surprisingly, businesses are beginning to follow suit as computer servers, network gear, corporate social media accounts, online systems for HR, payroll, data storage, business intelligence, banking and other functions all require a method of access. From fingerprints to facial recognition, businesses are grappling with the legal ramifications of this developing trend.

There are two important legal components to consider. First, there is an enhanced privacy compliance requirement. Second, businesses need to be attuned to the necessity of obtaining contractual protections and creating appropriate policies to protect corporate assets.

Privacy Requirement

More US states are enacting specific biometric privacy statutes that require additional privacy protections and disclosures whenever businesses use or store "biometric identifiers", which may include fingerprints, facial geometry, and retina and iris scans, among other things. Some of these state laws have been interpreted by the courts to apply even in the case of facial geometry derived from photographs, rather than directly from the individual.

Contractual Protections and Policies

Businesses need to take adequate steps to assure access to corporate resources, since a departing employee cannot turn in a copy of his or her face in the same way they turn in a badge on the last day of work. These steps should include policies to assure that there are alternative means of accessing critical data, and commitments by affected personnel to provide such access.

Blockchain Technology

Applications of blockchain technology exploded during 2017 and are expected to continue to accelerate into 2018. "Blockchain" refers to a variety of techniques, popularised for the bitcoin cryptocurrency, for maintaining a ledger of information consistently across multiple computers on a decentralised network. Applications include ledgers of finan-

cial assets, energy transactions on a grid, ingredient sources in a food products supply chain, and many others.

The privacy and data security issues related to blockchain technology can be complex. On one hand, blockchains can enhance privacy and security because they use encryption techniques for storage and access authorisation, and because they can sometimes be used anonymously or partially anonymously. On the other hand, they can deter privacy and security because they are built to be accessed across large, sometimes public, networks.

The technical claims about features of blockchains must be carefully scrutinised by lawyers. While blockchains are said to be decentralised and immutable, these descriptions are incomplete. Aside from the ever-present threat of hacking of any computer system, several highly publicised events have belied these features. On at least two occasions, on two different blockchains, a centralised group controlling the software of a blockchain was able to change the contents or function of a blockchain in order to correct a flaw. While those were beneficial changes, they make clear that blockchains can be changed in certain circumstances.

Regulatory developments are also rapidly occurring, particularly around blockchain financial and cryptocurrency applications, and any business preparing to deploy a blockchain should engage with legal specialists in order to avoid problems. At the federal level, securities, commodities and anti-money laundering regulations are being applied. Across the US, some states are encouraging the adoption of blockchains, while others are imposing additional regulatory burdens.

Malware

Malicious software – or "malware" – is a constantly evolving threat to computer safety and sensitive information. In many ways, however, malware is outpacing the contractual protections commonly used to protect against it. While contract provisions that address computer malware risk are commonplace in contracts for software and cloud computing, and in representations and warranties applicable to M&A transactions, those provisions have evolved little since their introduction.

Traditional anti-virus/anti-malware language addresses whether or not a virus is present *at the time of contracting*, and focuses on whether steps are taken to avoid the introduction of viruses. Common language generally does not address the resilience of a system to withstand the introduction of a new virus or other malware. It is also unusual for the scope of the language to encompass the increasing world of smart devices (including "internet of things" devices) in an enterprise.

In 2017, highly publicised data security incidents – such as "WannaCry" and the EquiFax breach – had in common the fact that the breaches resulted from failures to correct flaws that had been found and publicly reported before the event. In some cases, the breach was exacerbated by systems that were vulnerable to these threats but were not accessible to have the corrections applied. As a result, "failure to patch for known vulnerabilities" emerged as one of the most frequent root causes of reported breaches.

Modern, updated contractual provisions are evolving to address these issues. Contracts should assure that computer systems are *not* 1) dependent on software that no longer has appropriate security updates available, or 2) engineered to depend on software that cannot be updated in the future.

Beyond that, contracting parties should establish and implement processes for applying all necessary software updates to any potentially vulnerable system, not just those in the IT department.

EU-US Cross-Border Data Transfers

The regulation of cross-border transfers will change drastically in 2018, as the General Data Protection Regulation ("GDPR") is implemented in the European Union in May. Many US-based companies will find it difficult, if not impossible, to comply, as the historic EU legislation requires a level of discipline in data mapping, processing and transfer that is quite foreign to most US companies. The GDPR's very onerous penalties for non-compliance will create tremendous pressure for EU companies to demand that their US affiliates and contract counterparties bring themselves into compliance. As such, those whose houses are in good order and are able to meet the new standard will be in a very advantageous market position, as EU companies will need to look for new vendors and new partners to avoid the drastic financial penalties of the GDPR.

Regulation of the transfer of personal data from the EU to the US is not new. The EU Data Protection Directive (Directive 95/46/EC), adopted in 1995, and the national laws implementing it in each EU Member State, have always acknowledged that the data protection laws in the US are "inadequate" by EU standards, and have required EU companies to ensure that they meet one of several higher standards of care if they transfer data to US companies. However, many US companies remain unaware of these rules, and of what their EU contracts actually require. This will change with the GDPR, as the penalties will skyrocket to as much as 4% of annual turnover for non-compliance by the EU data transferor.

The US' first attempt at a "Safe Harbor" self-certification process for US companies was struck down by the European Court of Justice. The European Commission, the US De-

Contributed by McGuireWoods LLP **Authors:** Emilio Cividanes, Stuart P. Ingis, Michael Signorelli, Julia Kernochan Tama

partment of Commerce and the Swiss Administration then agreed on a new, stronger self-certification process for US companies, known as the "Privacy Shield." While the Privacy Shield could ultimately fail for the same reasons as the Safe Harbor, for now it is one of the limited options for EU-US cross-border data transfers. Self-certification requires US companies to submit to oversight by the Federal Trade Commission, to meet numerous, specific obligations, and to commit to a set of privacy principles for itself and for all of its contracted vendors who touch personal data. The specifics of self-certification under the Privacy Shield are found at www.privacyshield.gov.

US Data Breach Notification Statutes

In the United States, the federal government has imposed only limited regulations regarding notification of individuals in the event of a breach of their personal information. In the vast majority of US data breaches, the obligation of the data controller (or processor) to report the breach to the data subject depends on the laws of the *state of residence* of the data subject. Forty-eight of the 50 US states, together with the District of Columbia, Puerto Rico, the US Virgin Islands and Guam, have statutes governing data breach notification. Alabama and South Dakota currently have no data breach notification statutes.

McGuireWoods LLP
800 East Canal Street
Richmond, VA 23219-3916

Tel: (804) 775-1000
Fax: (804) 775-1061
Email: info@mcguirewoods.com
Web: www.mcguirewoods.com

Careful analysis of each state's definition of "personal information" is critical. While many states have a simple definition of the type of data that triggers a notification requirement (data subject's first + last name or first initial + last name combined with a driver's licence number, state ID number, or financial account number and PIN), others – like California and New York – have a much broader definition. Similarly, the definition of a "breach" varies widely from state to state. Most state statutes only cover data stored electronically, but some, like North Carolina, include breaches of data stored on paper. Some states have firm deadlines for notice, like Florida (30 days from determination of breach), while others require it "without unreasonable delay." Some states require notice to the State Attorney General, some dictate specific content of the notice letter, and still others have unique requirements. California requires the company to offer free identity-theft protection and mitigation services to the data subject for 12 months.

Myriad state laws and varying definitions make compliance difficult in a multi-state breach. Companies are well served by engaging experienced data breach counsel to analyse state breach notification requirements, and experienced vendors to assist with sending notices, offering credit monitoring and identity repair services, and providing telephone support for data subjects.