Privacy & Cybersecurity

Compliance programmes – the core of the debate

WilmerHale lead the global interview panel
market intelligence

Welcome to GTDT: Market Intelligence.

This issue focuses on privacy and cybersecurity.

Getting the Deal Through invites leading practitioners to reflect on evolving legal and regulatory landscapes. Through engaging and analytical interviews, featuring a uniform set of questions to aid in jurisdictional comparison, Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most interesting cases and deals.

Market Intelligence is available in print and online at www.gettingthedealthrough.com/intelligence.

Getting the Deal Through
London
August 2017

In this issue

- Global Trends ................................................................. 2
- Australia ........................................................................... 4
- Belgium and the European Union .................................. 10
- Brazil ............................................................................... 20
- China ............................................................................... 26
- Germany ......................................................................... 33
- Greece ............................................................................ 38
- Hong Kong ....................................................................... 45
- Mexico ............................................................................. 50
- Netherlands ..................................................................... 55
- Peru ................................................................................ 61
- Russia ............................................................................. 66
- United Kingdom ............................................................. 71
- United States ................................................................. 78
GLOBAL TRENDS

JASON CHIPMAN AND BENJAMIN POWELL OF WILMERHALE

WilmerHale special counsel Jason Chipman’s practice focuses on cybersecurity and data breach issues, in addition to advising clients about the Committee on Foreign Investment in the United States, Defense Security Service issues, and export control investigations and guidance. Jason has advised many global companies on how to navigate significant data security incidents and related privacy matters. He is also often called upon to help companies address regulatory issues associated with data security and handling. He joined the firm in 2011 after serving as senior counsel to the Deputy Attorney General at the US Department of Justice, and after having previously served as counsel for National Security Law and Policy in the Department’s National Security Division.

WilmerHale partner Benjamin Powell has advised companies on major cybersecurity incidents and incident preparedness across virtually every sector of the economy, including the banking, investment management, software, retail, energy, defense and intelligence, media and entertainment, pharmaceutical, cloud services, government contracting, aerospace, information technology, manufacturing, and travel sectors. He is recognised as a leading attorney in handling complex regulatory matters relating to international investment and mergers, including matters involving the Committee on Foreign Investment in the United States and the Defense Security Service.
Cybersecurity continues to represent a growing risk for companies around the world with cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and ‘hacktivists’ continuing to grow on a global basis. Recent high-profile and disruptive cyberattacks using ransomware have become particularly problematic for large and small companies alike. At the same time, criminal groups are increasingly attempting to use cyber hacks to extort money from victim companies. In this environment, maintaining an effective corporate cybersecurity programme is becoming the standard expectation for all businesses, and the ability to respond efficiently and effectively to data security emergencies will be important for avoiding potentially disruptive cybersecurity incidents in the future.

Many countries around the world are creating new regulatory requirements for businesses identified as possessing particularly important data meriting special protections. In the United States, it continues to be the case that dozens of federal and state statutes address cybersecurity issues, but no overarching statutory framework exists. The US Congress enacted legislation in late 2015 to encourage businesses to voluntarily share cyberthreat data with one another and with the government. In December 2016, the Commission on Enhancing National Cybersecurity, which was created by a presidential directive, issued more than 50 recommendations for improving cybersecurity in the United States. And in May 2017, President Trump issued a new cybersecurity executive order requiring US federal government agencies to take special measures to better protect government networks and government data. At the same time, US regulatory agencies are expanding enforcement actions to address cybersecurity issues.

In Europe, on 17 May 2016, the European Council adopted the Network and Information Security Directive, which imposes security obligations on ‘operators of essential services’ in certain important economic sectors, such as health, water supply, financial markets, banking and energy. Businesses in these sectors will be required to manage cyber risks and to report significant cyber breaches. Similarly, in April 2016 the European Parliament adopted the EU General Data Protection Regulation, which requires data processors to implement a variety of security provisions and to appoint data protection officers.

In China, a new cybersecurity law came into effect in June 2017 that imposes special data localisation requirements, personal data handling rules, and requirements to cooperate with law enforcement for businesses that handle critical infrastructure data and for network operators. The law allows for fines and other penalties for non-compliance.

For large global companies, these changing rules mean that cybersecurity standards may apply to some or all company operations (depending on economic sector) and that special handling rules are very likely to be implicated for the hosting and processing of sensitive data, such as personal data about consumers, critical infrastructure data and financial sector data. Cybersecurity will remain a major issue for such organisations and will continue to require technical, legal and communications experts to work together to manage the risk of data security incidents.
PRIVACY & CYBERSECURITY IN THE UNITED STATES
GTDT: What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Jason Chipman & Benjamin Powell: Although many economic sectors in the United States have little or no cybersecurity standards, there is a growing trend toward more prescriptive requirements in economic sectors perceived as playing a critical role in the US economy or for US security. For example:

- In the financial sector, companies are increasingly subject to mandatory cybersecurity standards imposed by state or federal authorities. On 1 March 2017, the New York State Department of Financial Services (NYDFS) enacted cybersecurity regulations for banks, insurance companies and other financial institutions subject to NYDFS jurisdiction.

- In the energy sector, commensurate with growing anxiety in the US about energy sector cybersecurity vulnerabilities, several recent regulatory initiatives focus on cybersecurity best practices. In April 2017, the North American Energy Reliability Corporation and the American Gas Association announced efforts to improve security collaboration on common threat information and incident response. And in May 2017, the US President issued an executive order mandating that the Departments of Energy and Homeland Security evaluate electrical sector resilience to respond to a significant cyber incident.

- In the defence sector, companies in the government contracting sector are subject to increasingly precise cybersecurity standards established by the National Institute of Standards and Technology.

For companies handling consumer data, the Federal Trade Commission (FTC), the main federal consumer protection agency responsible for enforcing the prohibition on ‘unfair and deceptive acts or practices’, frequently enforces minimum security requirements with respect to entities collecting, maintaining or storing personal information. In June 2015, the FTC issued ‘Start with Security’ guidance, which identifies the FTC’s lessons learned from over 50 data security enforcement actions it has brought since 2001. This guidance advises companies to incorporate a series of 10 lessons learned, ranging from authentication controls to network segmentations. Additionally, companies in the US that handle credit card data are subject to specific but privately imposed cybersecurity standards that are promulgated by the Payment Card Industry Security Standards Council.

Over time, we anticipate that pressure will continue to grow to establish more uniform and clear cybersecurity standards, but a consensus on how to craft such standards is likely to remain elusive. Federal agencies in the United States are likely to continue efforts to craft more aggressive cybersecurity regulatory requirements applicable to particular economic sectors, such as recent efforts to impose far-reaching cybersecurity standards on companies operating in the government contract and financial sectors. Legislative action in the near term will almost certainly steer clear of establishing mandatory cybersecurity requirements, and will instead focus on creating incentives for private sector entities to share cyberthreat data more freely with one another and with the government.
When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The US does not have a uniform data breach notification law. Rather, 48 US states and jurisdictions have individual data breach notification laws. At the federal level, sector-specific laws for government contractors, certain financial institutions and certain businesses handling health records also impose special breach notification rules. In general, data breaches mandate notification to regulators or consumers when specific categories of sensitive personally identifying information are compromised through a cyber intrusion, inadvertent disclosure or other loss of electronic data. For example, in many jurisdictions the unauthorised acquisition of data that includes names combined with social security numbers, financial account numbers, health records or passport numbers would trigger a mandatory breach notification obligation to the consumer and may also trigger such a notification to a state attorney general or to another regulatory body.

What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Data security incidents, particularly cyber intrusions, may trigger several different and significant challenges. For companies handling substantial amounts of sensitive personal information, such incidents may trigger:

- communications challenges for companies that want to provide consumers or other customers with reassurance while also investigating the scope of a particular incident;
- remediation challenges in taking steps to further safeguard sensitive data to both stop a cyber intrusion and to help bolster existing security; and
- investigative challenges to determine the scope of the intrusion, what data was taken and whether the attacker has been removed from the company networks.

Managing these sorts of challenges, often while also coordinating with law enforcement authorities or other regulators, requires all components of a business to work together. Such incidents are not just the province of the information technology team; they are problems that require senior attention to manage and address.

What best practices are organisations following to improve cybersecurity preparedness?

Incident response requires an immediate, coordinated effort to gather the facts through forensic analysis and to execute an incident response plan that enables the company to address multiple work streams simultaneously in a coordinated fashion. The response generally prioritises remediation, reputational harm, communication with all the relevant constituencies (including, critically, customers) and preparing for the range of potential regulatory inquiries and litigation that may follow.

Companies can take several steps to best prepare for improving their ability to respond to such issues, such as:

- reviewing existing incident response plans, benchmarking against industry best practices, and proposing changes;
- developing and participating in tabletop exercises to help those with implementation responsibilities understand how the incident response plan would work in practice;
- engaging third-party firms in advance, through counsel, to ensure that the right resources are available to address critical issues in a time sensitive manner;
- reviewing incident response plans on an annual basis to determine if revisions are warranted. Plans should also be reviewed after any serious incident to incorporate lessons learned from the company’s response to that incident; and
- providing regular updates on, and analysis of, legal and regulatory developments that would influence response plans and practices.

Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud services trigger a variety of risks that should be carefully balanced as part of the decision to outsource data storage or other information technology functionality.
Although cloud computing is somewhat new for many organisations, the risks associated with cloud computing are similar to other types of IT outsourcing. Those risks include:

- **Third-party access to data:** when company information is outsourced for storage or other processing by third parties, that information may no longer be solely within the control of the information owner. The cloud provider may be compelled to release it to third parties in litigation or to government agencies inside or outside the United States. Moreover, absent appropriate prohibitions in the parties’ agreement, a cloud provider may be entitled to share customer data (or data derived from customer data) with third parties for the cloud provider’s own business purposes.

- **Data security:** evaluating the security of data in a cloud environment and ensuring the use of appropriate safeguards can be very challenging. Many cloud providers will not provide full visibility into their own network security posture.

- **Location of data:** data entrusted to a third party may be stored or otherwise processed in a jurisdiction that gives rise to unique legal or regulatory concerns. Moreover, some cloud providers do not provide transparency or assurances concerning where the data will be located.

- **Privacy and consumer notice:** processing of consumer data by a third-party cloud provider may necessitate special notices to consumers or employees, and it may trigger a number of privacy and data protection obligations with respect to how their data will be handled, retained and distributed.

- **Business continuity and provider lock-in:** cloud providers and sub-processors may go out of business or otherwise experience a disaster or other incident that results in the loss, corruption or temporary inaccessibility of their customers’ data. Further, it may be difficult to extract data from a software-as-a-service (SaaS) solution at the end of the parties’ engagement, at least in a format that does not require substantial processing before the data can be ingested into a competitor’s SaaS product.

There is a wide range of different regulatory regimes that impact cloud outsourcing. Some regulations that are agnostic about whether data is outsourced in a cloud environment or remains within a company’s firewall impose general obligations that have the effect of imposing rules that data owners must satisfy in a cloud scenario (such as National Institute of Standards and Technology requirements to track and specially secure sensitive data). And other regulations are cloud-specific, such as ISO 27017, an independent security standard that provides guidance on the information security aspects of cloud computing.

### THE INSIDE TRACK

**When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?**

Legal advice around cybersecurity issues requires counsel that is experienced at addressing and managing the wide range of issues that cybersecurity incidents and related preparation activities may trigger.

**What issues in your jurisdiction make advising on privacy and cybersecurity complex or interesting?**

Cybersecurity is an evolving and changing field that requires lawyers to provide a mix of legal, policy and business guidance to clients navigating new and often challenging issues.

**How is the privacy landscape changing in your jurisdiction?**

Privacy is becoming a critical part of contracting arrangements between parties, with greater focus on compliance with state, national and international laws. Greater regulation of the handling, securing and transfer of data is resulting in an increasing focus by companies on privacy issues, particularly on specifying the obligations that must be met in the handling of data between parties. This trend will only increase with new regulations coming into force in the United States, the European Union and other countries.

**What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?**

There is an increasing understanding of cyberthreats in the US. High-profile incidents involving espionage and criminal actors receive frequent public attention, and companies need to be constantly on guard for the latest threats. In the recent past, incidents involving tax fraud were on the rise, and today ransom and extortion demands associated with cyber intrusions are becoming more common.

Jason Chipman and Benjamin Powell
WilmerHale
Washington, DC
www.wilmerhale.com
and is often used by organisations to judge their ability to manage data in a cloud environment.

**GTDT: How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?**

**JC & BP:** Cybersecurity is increasingly a substantial focus of federal and state law enforcement efforts in the US. The Federal Bureau of Investigation (FBI) has grown its cyber capabilities substantially over the past several years and Congress is increasingly focused on finding the necessary resources to combat cyber espionage, cybercrime, and other forms of improper cyber activity. Specific laws that address criminal activity in the cyber context include the Computer Fraud and Abuse Act, which outlaws intrusions into or interference with the security of a government computer network or other computers connected to the internet. In addition, several federal surveillance laws prohibit unauthorised eavesdropping on electronic communications, which can limit a variety of cybersecurity activities. For example, the Electronic Communications and Privacy Act prohibits unauthorised electronic eavesdropping. The Wiretap Act prevents the intentional interception, use or disclosure of wire, oral or electronic communication, unless an exception applies. The Stored Communications Act precludes intentionally accessing without authorisation a facility through which an electronic communication service is provided and thereby obtaining, altering or preventing authorised access to a wire or electronic communication while it is in electronic storage.

**GTDT: When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?**

**JC & BP:** Cybersecurity and privacy is increasingly a significant topic for M&A due diligence because of potential regulatory or litigation exposure that a company may acquire through an acquisition. Acquirers often seek special assistance today to evaluate the scope of exposure by examining the nature of the target business, the type of data it maintains about customers or third parties, and the regulatory environment in which it operates.