THE INVESTIGATIONS REVIEW OF THE AMERICAS 2018

Published by Global Investigations Review in association with:

Blake, Cassels & Graydon LLP
Campos Mello Advogados
D'Empaire Reyna Abogados
EY
Herbert Smith Freehills
Hogan Lovells
Kirkland & Ellis LLP
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados
Miller & Chevalier Chartered
Mitrani Caballero Ojam & Ruiz Moreno
Morrison & Foerster
Sidley Austin LLP
Sullivan & Cromwell LLP
Weil, Gotshal & Manges LLP

GIR
Global Investigations Review
www.globalinvestigationsreview.com

The Investigations Review of the Americas 2018

A Global Investigations Review Special Report

The Investigations Review of the Americas 2018

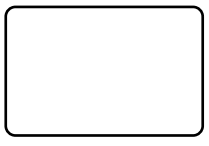
Senior co-publishing business development manager George Ingledew
Senior co-publishing manager Edward Perugia
edward.perugia@globalinvestigationsreview.com
Tel: +1 202 831 4658

Head of production Adam Myers
Editorial coordinator Iain Wilson
Chief subeditor Jonathan Allen
Production editor Caroline Herbert
Subeditor Simon Tyrie

Editor, Global Investigations Review David Vascott
Editor in chief David Samuels

Cover image credit: iStock.com/blackdovfx

Subscription details
To subscribe please contact:
Tel: +44 20 3780 4242
Fax: +44 20 7229 6910
subscriptions@globalinvestigationsreview.com



ISSN: 2056-6980

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

The Investigations Review of the Americas 2018

Published in association with:

Blake, Cassels & Graydon LLP

Campos Mello Advogados

D'Empaire Reyna Abogados

EY

Herbert Smith Freehills

Hogan Lovells

Kirkland & Ellis LLP

Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Miller & Chevalier Chartered

Mitrani Caballero Ojam & Ruiz Moreno

Morrison & Foerster

Sidley Austin LLP

Sullivan & Cromwell LLP

Weil, Gotshal & Manges LLP

Contents

Cross-border overviews

Enforcer overviews

Country chapters

Cyber breach notification requirements

Stephanie Yonekura, Eduardo Ustaran and Allison Bender
Hogan Lovells

Global companies with a multinational base of consumers, employees and operations face myriad data protection laws, now enacted in almost 100 countries. California's S.B. 1386, enacted in 2002 and effective 1 July 2003, was the first data breach notification law. Since then, requirements to notify affected individuals and government authorities of a breach of personal information have been enacted widely across the United States and have been increasingly adopted internationally.[1] Data breach notification laws generally apply based on the residence of the potentially affected individuals, not the location of the data breach, nor the base of a company's business operations.

While the underlying obligation to notify is the common theme for this accelerating legal trend, these laws may differ widely in defining what data may be considered personal information; what events may be considered a breach; when the obligation to notify may be triggered; to whom notifications must be sent; the timing, format, contents and method of such notifications; and the penalties and rights of action for non-compliance. The recent spate of ransomware attacks have also created high-level concern across the globe among businesses seeking to confirm that they are prepared for a ransomware attack, as well as other types of cyberattacks. Even within the same jurisdiction, a ransomware attack may be considered a 'breach' and trigger notification obligations under one set of applicable legal requirements; whereas under other laws, it may not rise to the level of a 'breach' by definition or it may fall within an exception, such as for limited risk of harm or encryption, for otherwise applicable data breach notification obligations. Additionally, numerous jurisdictions that have not enacted such requirements nevertheless have issued strong guidance encouraging voluntary notifications and/or maintenance of internal registers of data security incidents.

While the United States has developed a significant body of law with respect to mandatory data breach notification since the first law in California, the European Union (EU) General Data Protection Regulation (GDPR), set to become applicable 25 May 2018, is likely to intensify requirements for companies to prepare well in advance for an EU or cross-border data breach. Article 33 of the GDPR requires a company that is a data controller to notify data protection authorities of a personal data breach 'without undue delay and, where feasible, not later than 72 hours after having become aware of it,' and pursuant to article 34, with limited exceptions, to notify affected individuals 'without undue delay' '[w]hen the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.' While countries like China and Australia have also recently adopted mandatory data breach notification regimes, this article focuses on nuances in the existing US and upcoming EU data breach notification laws to assist practitioners in mitigating and investigating cross-border data incidents subject to these requirements.

United States

In the United States, 48 states,[2] the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws that require notification of data breaches that involve certain types of personal information. These state breach notification laws vary, but generally require notification when there has been 'unauthorised acquisition of',[3] 'access to',[4] or 'a reasonable belief of unauthorised acquisition of'[5] personal information.[6]

The majority of state breach notification laws define 'personal information' (or an equivalent term) to include names plus certain unencrypted sensitive data elements (eg, social security number, government identification numbers, financial account or payment card information, health information).[7] In addition, seven states – California, Florida, Illinois, Nebraska, Nevada, Rhode Island and Wyoming – have defined 'personal information' to include a username or email address in combination with a password or security question and answer that would permit access to an online account.

The term 'unauthorised acquisition' (and similar variants) is not defined under the various state laws, but is understood to involve more than mere 'access' (eg, access involves viewing or having the ability to view or access a file without actually downloading, printing, copying electronically, or copying manually). New York's statute and California's informal breach guidance include examples of unauthorised acquisition:

- indications that the information is in the physical possession and control of an unauthorised person, such as a lost or stolen computer or other device containing information;
- indications that the information has been downloaded or copied; or
- indications that the information was used by an unauthorised person, such as fraudulent accounts opened or instances of identity theft reported.[8]

However, there are some states that define 'breach' in terms of mere unauthorised access to personal information, rather than requiring that there be acquisition.[9] In these states, breach notification obligations may exist, even without exfiltration. Those states are Connecticut, Florida, New Jersey and Rhode Island. Looking at the definitions of personal information in these states, at least in Florida and Rhode Island, unauthorised access to an account username and password alone would be sufficient to trigger notification obligations. Additional states' notification obligations may be triggered if the nature of the username and password information was related to a financial account, for example, or if the data accessed without authorisation included other types of personal information.

For states that require notification only upon unauthorised acquisition (as opposed to mere access), further investigation is necessary to determine whether data was actually exfiltrated (or reasonably likely to have been exfiltrated). If data was indeed exfiltrated, then the investigation will turn first to determine the nature of that data and second to ascertain the states of residency for the individuals about whom the data relates. To determine whether data was exfiltrated, forensic examination of affected systems is likely to be required. This may include, for example, reviewing available logs,

and if the log analysis does not provide sufficient detail to assess this key question, reviewing the contents of the affected devices to determine the type of data potentially affected. If personal information, generally as defined in the law of the state of residency for each affected individual, was reasonably likely to have been exfiltrated, then that state's general data breach notification law is likely to be triggered. Depending on the residency of each individual affected, applicable state law may also require notification to state government authorities if even one resident is affected or if a threshold total of state residents are affected.

Thirty-nine[10] states' breach notification laws do not require notification to individuals if the organisation determines that the incident does not pose a risk of harm to the affected individuals. The risk of harm standard varies among the states. A number of states' laws refer generally to the risk of misuse of the personal information, while other states' laws refer more specifically to the risk of identity theft, fraud or economic loss. Some states require law enforcement to be consulted in making this determination. Also, some states require written documentation of the risk-of-harm analysis to be submitted to the state regulator if notice will not be made due to the conclusion that there is no risk of harm.

Certain states have moved from simply requiring notice of breaches after they happen towards setting out more prescriptive standards aimed at prevention of data breaches. At least 12 states – Arkansas, California, Connecticut, Florida, Maryland, Massachusetts, Minnesota, Nevada, Oregon, Rhode Island, Texas, and Utah – impose various levels of data security requirements on businesses that collect personal information about residents of that state.[11] While there are some variations, generally these laws do not contain many specific data security requirements, instead requiring only that businesses implement and maintain 'reasonable' procedures to safeguard personal information.[12] Some states require businesses that contract with third-party service providers to take additional steps to ensure the security of the data transferred to those providers.[13]

The most detailed of the state information security laws is the Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts (the Massachusetts Standards).[14] The comprehensiveness of the Massachusetts Standards has led many companies to view those standards as a reasonable proxy for compliance with other information security legal standards in the United States.

European Union

The GDPR is a regulation under EU law, meaning that, when it takes effect, it will apply directly in all 28 member states of the EU. Consequently, there will be no need for EU governments to implement the GDPR locally and existing national data protection law will ultimately need to be repealed to make way for the GDPR. While individual member states can implement derogations from the GDPR requirements, any such derogations are expected to be much more limited in scope, meaning that the consistency of data protection requirements across member states is likely to be enhanced under the GDPR. Additionally, the Data Protection Directive 95/46/EC (the Directive) will be repealed on the day the GDPR becomes law.

Existing data protection authorities in each of the member states will keep their supervisory role but will be given more powers. This includes a power to fine organisations (controllers and processors) up to 2 per cent of total worldwide annual turnover for the failure to notify data protection authorities and individuals, as may be required under articles 33 and 34. Additionally, a new European Data Protection Board (an updated version of the current Article 29 Working Party under the Directive) will play a much greater role with wider powers in ensuring the consistent application of the GDPR across the EU.

More organisations are subject to the GDPR than were subject to the Directive. Specifically, under the GDPR, processors will be subject to direct legal obligations (although not as wide-ranging as the obligations on controllers). Processors are organisations that act as service providers and only process data because another organisation (a controller) has engaged them to do so on their behalf. Additionally, organisations that are not established in the EU but offer goods or services to individuals in the EU or monitor their behaviour will also be required to comply with the GDPR. As such, a company based in the US or Asia, for example, which nevertheless has a consumer base that includes EU-based individuals, will be expected to comply.

Similarly to the Directive, certain information must be provided to individuals to explain the context for the use of their personal data. However, the GDPR expands the list of what individuals need to be told to include information, such as whether data will be transferred, how long it will be kept for, and information about any profiling individuals will be subject to. Similar information must be provided to individuals by an organisation where the organisation has not collected the data directly from the individual. Unlike in the United States where a 'breach' is typically an unauthorised access to or acquisition of covered personal information, under the GDPR, a breach is 'the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.' As such, more data security incidents may be considered a 'breach' under GDPR, ransomware included.

Controllers will be under specific obligations to introduce data protection by design and default into their processing systems when building databases and systems. This obligation underscores the need for organisations to consider data protection compliance at the start of a project so that data protection rules can be integrated.

Data protection impact assessments (DPIAs) are mandatory where proposed data processing is likely to result in a high risk to the rights and freedoms of individuals. DPIAs will help a company prepare for, prevent against, and mitigate the consequences of a data breach. A DPIA involves an assessment of the likelihood and severity of the risks involved in the proposed data processing, as well as the measures and safeguards to be introduced to mitigate the risk. Large-scale processing operations affecting many people that are likely to result in a high risk will require a DPIA.

Both controllers and processors will be under new obligations about the documentation they must retain and the provisions their contracts must include. Controllers will need to implement appropriate data protection policies, and both controllers and processors will be required to keep a record of processing activities. The GDPR specifically sets out the provisions that must be included in controller-processor contracts.

The GDPR introduces an obligation to report data breaches to data protection authorities and, in some cases, to affected individuals. This is a new comprehensive obligation that is not industry-specific but instead is triggered if the personal data breach is likely to result in a risk to individuals. This obligation to notify affected individuals is only triggered where the breach could result in a high risk to individuals, and a controller does not need to notify individuals if the data that is the subject of the breach has been subject to certain measures, such as encryption, that make it unintelligible to

unauthorised recipients; the controller has taken measures to reduce the risk; or if notification would involve a disproportionate effort.

The nature of incident response and data breach investigations is such that it may be difficult for a company to determine whether in fact a breach, as defined by law, has occurred. In the United States, typically the time frame for making required notifications is based on when the organisation determines that a breach has occurred, not merely when it became aware of an incident. In the first 72 hours after discovery of an incident, it may not be possible to conduct the necessary forensics to determine whether, in fact, the events amount to a breach. This potential interpretation of the GDPR's article 33 requirement may result in more 'false positive' data breach notifications in the EU than in the United States; but it also will provide a speedier notification in all cases and set a clear time frame as the bar for compliance, unlike the US laws' typical requirement of notifications following a 'reasonable investigation.' As such, preparing for a data breach and ensuring adequate capability and effective processes to be able to respond to an incident and execute any GDPR-required notifications in a prompt manner will be critical for companies' compliance.

One additional area that is given greater prominence in the GDPR is adherence to codes of conduct to demonstrate compliance. Data protection authorities are to encourage the development of codes to take account of the specific features of particular industries and sectors. Where a data protection authority approves a code, adherence can be relied upon by organisations to demonstrate compliance with other aspects of the GDPR. (Consequently, industry sectors may explore developing a code tailored for their specific requirements.) A similar means of demonstrating compliance exists if a controller or processor obtains a certification that is recognised under the GDPR. It remains to be seen whether any of the standards or guidance frameworks developed by various national and international standards bodies, government agencies and trade organisations may be recognised as a code of conduct or certification, which may be used to evidence GDPR compliance.

Conclusion

A company affected by a data security incident, which involves the personal information of a broad group of residents of various jurisdictions, faces a substantial burden to analyse all potential legal requirements, based on the laws of the jurisdictions in which affected individuals are residents, in considering whether and how to make notifications. As a result, such companies may elect to notify the entire group of individuals affected. This has benefits in reducing the analytical burden, because electing to notify broadly reduces the amount of legal analysis necessary to avoid 'over-notification' in jurisdictions where notification may not be required. Instead, if data breach notification is required in any jurisdiction or a significant number of jurisdictions, the company's decision to elect to notify the broader group of affected individuals will allow the focus of incident and data breach response efforts to shift to ensuring prompt notification, with consistent messaging. If any notification may be required, promptness and consistency aid in perception management, potentially reducing the risk of litigation and reputational harm to the company, regardless of jurisdiction. Depending on a company's consumer base, geographic scope of business operations, applicable laws and regulations, and the specific facts in an incident, it may be possible for a company to 'dance through raindrops without getting wet,' but the global trend towards the adoption of data breach notification requirements will make it less likely that a company may avoid notifications altogether.

Companies can prepare in advance by developing a holistic, enterprise-wide incident response plan; engaging in periodic cybersecurity exercises to test such plans and the capabilities of the company to respond; and monitoring legal developments as data breach notification laws continue to spread. Companies with EU-facing operations are likely to benefit across jurisdictions from conducting the required DPIA to assess their risks and may also benefit from participating in industry-specific efforts to develop codes of conduct that help fill in the details of GDPR compliance in a manner that aims to harmonise GDPR compliance with existing data breach notification obligations across other jurisdictions.

Notes

1 Industry-specific regulations, such as those relating to health, energy or the financial sector may also apply, but discussion of these specific regulations goes beyond the scope of this chapter.

2 New Mexico's law was enacted this year and became effective on 16 June 2017.

3 See, eg, TEX. BUS. & COM. CODE § 521.053.

4 See, eg, N.J. STAT. § 56:8-161.

5 See, eg, ALASKA STAT. § 45.48.090(1).

6 Some state statutes use close variants of the terms 'unauthorised acquisition' and 'unauthorised access,' such as 'unauthorised access and acquisition', 'unlawful and unauthorised acquisition', 'unauthorised acquisition or acquisition without valid authorisation', and 'unauthorised acquisition or unauthorised use'.

7 A few states' definitions of personal information do not require a name in combination with one or more sensitive data elements; rather, an unencrypted sensitive data element on its own meets the definition of personal information. For example, in Indiana, 'personal information' means either (i) a social security number that is not encrypted or redacted; or (ii) an individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted: (i) driver's licence number; (ii) state identification card number; (iii) credit card number; or (iv) a financial account number or debit card number in combination with a code or password that would permit access to the person's account.

8 See N.Y. GEN. BUS. LAW § 899-aa(1)(c); CAL. DEP'T OF CONSUMER AFFAIRS, OFFICE OF PRIVACY PROTECTION, RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 11 (January 2012).

9 See, eg, CONN. GEN. STAT. § 36a-701b(1); FLA. STAT.§ 501.171(1)(a).; N.J. STAT. § 56:8-161; R.I. GEN. LAWS § 11-49.3-3(1).

10 This count includes New Mexico, whose breach notification statute became effective in June 2017.

11 Ark. Code Ann. § 4-110-104(b); Cal. Civ. Code § 1798.81.5; Conn. Gen. Stat. § 42-471; Fla. Stat. § 501.171(2); Md. Code Ann., Com. Law § 14-3503; 201 CMR 17.00; Minn. Stat. 325E.64; Nev. Rev. Stat. Ch. 603A; Ore. Rev. Stat. 646A.622; R.I. Stat. 11-49.2-2; Tex. Bus. & Com. Code Ann. § 521.052; Utah Code Ann. § 13-44-201.

12 See eg, Tex. Bus. & Com. Code Ann. § 521.052(a).

13 For example, under the Maryland Personal Information Protection Act, a business that discloses personal information to a third-party service provider must contractually require the third-party to implement and maintain reasonable security

procedures and practices. Other states, such as Minnesota, call for companies that use payment card readers to comply with at least part of the Payment Card Industry Data Security Standard (PCI-DSS). Nevada requires that companies encrypt sensitive personal information if transferred.

14 201 CMR 17.00; See also Commonwealth of Ma. Off. of Cons. Affairs and Bus. Reg., Frequently Asked Questions Regarding 201 CMR 17.00, www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf.

Stephanie Yonekura
Hogan Lovells

Stephanie brings a unique perspective to any internal investigation. Having served as the Acting US Attorney in Los Angeles, she knows the hot-button issues that are considered in every stage of any government investigation.

As the Acting US Attorney of the largest office outside of Washington, DC, Stephanie was an active participant in the larger Department of Justice community, serving on nationwide committees on white-collar fraud, cybercrime, and intellectual property. Stephanie interacted with corporations when they were under investigation as well as when they were victims of crimes.

Stephanie worked with the FBI, SEC, IRS, CFTC, and various inspectors general as a prosecutor for more than 14 years, on issues including financial institution fraud, government fraud, securities fraud, and cybercrime. She developed a strong reputation with the court, defence counsel, and investigating agencies for digging into the facts and collaborating with law enforcement agencies and victims. She was also known for her ability to streamline investigations and make fair and equitable charging and sentencing decisions. In the courtroom, Stephanie exudes confidence, knowledge, and integrity.

In private practice, Stephanie uses her extensive experience in the trenches, in the courtroom, and as the chief law enforcement officer in Los Angeles to help clients understand the key issues and investigate matters strategically. She has represented companies around the world in FCPA, False Claims Act, anti-money laundering, securities, cybersecurity, and other government regulatory matters.

Hogan Lovells

1999 Avenue of the Stars
Suite 1400
Los Angeles CA 90067
United States

Stephanie Yonekura
stephanie.yonekura@hoganlovells.com
Tel: +1 310 785 4668

Eduardo Ustaran
eduardo.ustaran@hoganlovells.com
Tel: +44 20 7296 5249

Allison Bender
allison.bender@hoganlovells.com
Tel: +1 202 637 5721

www.hoganlovells.com

Hogan Lovells is a global law firm. Our 2,500 lawyers on six continents provide practical legal solutions wherever our clients work takes us.

Change is happening faster than ever, and to stay ahead, our clients need to anticipate what's next. Legal challenges come from all directions. We understand and work together with our clients to solve the toughest legal issues in major industries and commercial centers around the world. Whether they're expanding into new markets, considering capital from new sources, or dealing with increasingly complex regulation or disputes, we can help.

A fast-changing and inter-connected world requires fresh thinking combined with proven experience. That's what we provide. Progress starts with ideas. And while imagination helps at every level, our legal solutions are aligned with our client's business strategy. Our experience in cross-border and emerging economies gives us the market perspective to be a global partner. We believe that when knowledge travels, opportunities arise.

About our investigations, white-collar and fraud practice:

Regulatory investigations. Allegations of fraud, bribery, and corruption. Sanctions and money laundering. Whistleblower complaints. Dawn raids. Multinational corporations and their executives face a growing range of threats to their business and reputations. If you get hit, you're going to need a strong investigative team. We work with our clients to manage the issues and limit the impact on their business.

Our strength lies in managing the overall impact – often with a multi-jurisdictional element. Our award-winning team handles asset recovery and issues relating to enforcement, whistleblowing, bribery and corruption investigations, criminal liability, regulatory violations, and tax investigations. We are adept at pursuing claims against a company's executive board, and we can implement internal policies and compliance programmes.

Local matters often give rise to international legal risk and investigations. Our team is experienced in handling cross-border work, including offshore jurisdictions. We know what is required to handle such issues, having worked in China, Russia, Europe, the Americas, Africa and the Middle East, freezing assets, or managing the interplay between foreign corruption and local jurisdictions. Our team has been there.

Eduardo Ustaran
Hogan Lovells

As a partner in the global privacy and cybersecurity practice of Hogan Lovells, Eduardo Ustaran is internationally recognised in privacy and data protection law. He is a dually qualified English solicitor and Spanish abogado based in London. Eduardo is also the author of *The Future of Privacy* (DataGuidance, 2013), a groundbreaking book where he anticipates the key elements that organisations and privacy professionals will need to tackle to comply with the regulatory framework of the future. Eduardo advises some of the world's leading companies on the adoption of global privacy strategies and is closely involved in the development of the new EU data protection framework. He has been named by *Revolution* magazine as one of the 40 most influential people in the growth of the digital sector in the UK, and is ranked as a leading privacy and internet lawyer by prestigious international directories.

Eduardo is a former member of the board of directors of the IAPP, co-founder and editor of *Data Protection Law & Policy*, and a member of the panel of experts of *Data Guidance*. Eduardo is executive editor of *European Privacy: Law and Practice for Data Protection Professionals* (IAPP, 2011), and co-author of *Beyond Data Protection* (Springer, 2013), *E-Privacy and Online Data Protection* (Tottel Publishing, 2007), and of the *Law Society's Data Protection Handbook* (2004). Eduardo has lectured at the University of Cambridge on data protection as part of its Masters of Bioscience Enterprise, and regularly speaks at international conferences.

Allison Bender
Hogan Lovells

Allison Bender advises clients on cybersecurity matters, including preparedness, incident response, transactions, information sharing, engagement with law enforcement, and public policy.

Before joining Hogan Lovells, Allison served as a cybersecurity attorney at the Department of Homeland Security (DHS), where she advised the Office of Cybersecurity & Communications on cybersecurity law and policy. Allison brings key experience in incident response as well as cybersecurity policy, export controls, information sharing, liability, and incentives. She was primary operational legal counsel for the federal response to the Heartbleed vulnerability, the USIS-KeyPoint data breach, and the Healthcare.gov data breach. She also provided primary counsel to DHS and interagency initiatives to implement Executive Orders 13636 and 13691 as well as Presidential Policy Directive 21. Her leadership experience includes serving as chair of the Automated Indicator Sharing Privacy & Compliance Working Group.

Before focusing on cybersecurity at DHS, Allison negotiated complex, international and domestic multimillion-dollar research and development agreements in emerging science and technology areas. She served as chief negotiator for the US government on nine legally binding international agreements. She led the oversight of over US$1 billion worth in DHS activities, leading compliance programmes for export controls as well as treaty and regulatory compliance. Allison also spent four years as primary counsel for the SAFETY Act, providing legal advice on legislation that protects companies with anti-terrorism technologies, laying the groundwork for many of the policies and procedures for its current operation.

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISSN 2056-6980