The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 2
(published in November 2015 – editor Alan Charles Raul)

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor

Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, Felicity Bown, Joel Woods

ACCOUNT MANAGER
Jessica Parsons

PUBLISHING MANAGER
Lucy Brewer

MARKETING ASSISTANT
Rebecca Mogridge

EDITORIAL ASSISTANT
Sophie Arkell

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Gina Mete

MANAGING DIRECTOR
Richard Davey

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK
© 2015 Law Business Research Ltd
www.TheLawReviews.co.uk
No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of November 2015, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above. Enquiries concerning editorial content should be directed to the Publisher – gideon.roberton@lbresearch.com

ISBN 978-1-909830-75-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INTERNATIONAL INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ADVOKATFIRMAET SIMONSEN VOGT WIIG AS

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K.

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JUN HE LAW OFFICES

LEE & KO

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

PEARL COHEN ZEDEK LATZER BARATZ

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

Cybersecurity turned out not to be, after all, the privacy issue of the year. Rather, the decision of the Court of Justice of the European Union (CJEU) to invalidate the US-EU Safe Harbor Framework was the blockbuster development of 2015. On 6 October, the CJEU struck down Safe Harbor as an approved mechanism for the transfer of personal data from the EU to the United States. The Court found that the European Commission had not properly assessed the 'adequacy' of the US legal regime for data protection, neither in 2000 when the Safe Harbor Framework was first agreed, nor subsequently. The basis for the Court's concerns stemmed from allegations that the United States engaged in 'indiscriminate' surveillance for national security reasons, and that such surveillance could mean that data protection for information transferred there might not be 'essentially equivalent' to protection in the EU.

'Equivalence', then, is the challenge of global privacy law today. Data localisation mandates imposed in Russia, in particular, but also surfacing as a possibility in other jurisdictions, like Brazil, are threatening international data flows and impeding digital trade. Indeed, the EU's stringent restrictions against data transfers to the United States are themselves a significant manifestation of data localisation. With luck and goodwill, a new US-EU Safe Harbor 2.0 will be negotiated and put in place quickly, and other mechanisms to authorise international data transfers – such as EU Model Contract Clauses and binding corporate rules – will remain available. Moreover, perhaps the EU will even acknowledge that US checks and balances on government surveillance, and the privacy protections enforced by the Federal Trade Commission (FTC), the Federal Communications Commission, 50 plus state attorneys general and numerous other federal and state agencies are least substantially equivalent to those of the EU – especially with regard to government surveillance!

1 Alan Charles Raul is a partner at Sidley Austin LLP.

The other big privacy story of 2015 is the 'nearly baked' status of the proposed General Data Protection Regulation in the EU. The replacement of the existing framework Directive, dating back to 1995, with a new Regulation will mean that privacy law in the EU will be uniform in text (rather than implemented in various formats in each Member State's national law, as is the case today). The new Regulation, which is likely to be approved around the beginning of 2016, will also be subject to more consistent, coordinated interpretation and enforcement, and may impose both stricter standards and higher penalties for violations (and is likely to include enforcement via 'collective redress', a possible EU version of US class actions). In addition, the Regulation will finally bring the EU into line with US-style data breach reporting. Adapting international privacy compliance programmes to the new Regulation will surely need to be an important priority for global organisations beginning in 2016 (to be prepared for the Regulation's eventual effective date).

In the United States, a court of appeals decided in the *Wyndham* case that the FTC was authorised to enforce reasonable data security standards under its broad power to prohibit 'unfair or deceptive' business practices. This decision was a major development because it confirmed the FTC's authority over cybersecurity and personal information data breaches under the agency's general consumer protection power. Additionally, the FTC was permitted to litigate against a company that was itself the victim of a criminal hack, even though the FTC has not published any applicable standards defining what constitutes 'reasonable' or otherwise legally required cybersecurity standards.

Cybersecurity information-sharing legislation may finally be enacted after having been stalled for almost two years in the US Congress, and numerous government entities have announced new guidance and expectations regarding data security, including the Department of Justice, the Securities and Exchange Commission, state regulators and a variety of other agencies, and there have also been a number of significant court decisions involving major retailers and other parties involved in breaches. A number of states have further tightened their data security and data breach reporting requirements. All of these developments have led many US companies to initiate internal reviews of their cybersecurity governance and readiness programmes.

Significant privacy and data security developments are also taking place around the rest of the world. In particular, new data breach reporting obligations are taking root in many countries. New or significantly revised privacy laws have been adopted in a number of countries. In Japan, for example, revisions to its privacy law will apply to international data transfers and to big-data applications, online direct marketing and other matters. In Brazil, the fallout from the Snowden leaks continues, and the government is still implementing the 2014 Internet Act, which enhances privacy rights over personal and behavioural data. However, the mandatory data localisation provisions to store Brazilian-sourced data only on servers physically located in the country have been dropped. In Russia, much debate has gone back and forth regarding the new legal obligations to store the data of Russians on local servers, but the ultimate resolution appears to permit the same information also to be stored outside the country.

Like numerous other countries, the Republic of Korea has amended its privacy law to increase potential penalties and continue aggressive enforcement of data breach and other violations. In Hong Kong, new privacy guidance has been provided for international

data transfers, surveillance tools like CCTV, and for collection and use of biometric data. Singapore has also amended its privacy law significantly, and included new provisions and guidance regarding marketing, data breaches and securing electronic data.

Some countries, like Turkey, have been considering adoption of new privacy laws based on the EU's 1995 Data Protection Directive. In the meantime, Turkey has adopted laws on processing personal data and privacy protection in the telecom sector, and established new requirements for e-commerce. Israel has seen the development of new guidelines regarding the use of cloud services in the financial sector.

China, too, has been debating whether to follow the US or EU model. No final approach has been decided, but the practice to date represents a mix of both. For example, personal privacy is expressly protected in a 2010 'Tort Liability Law,' as it would be under the US model. Government rules, judicial consideration, corporate practices and public expectations about privacy and data protection are changing fast. Administrative guidance has recently been issued on cloud computing and big data, and new policies are expected on e-commerce and internet law. Most significant, for the rest of the world, are draft provisions that could require mandatory data localisation for telecom operators and internet service providers, obligating them to retain users' data in China, as well as possibly requiring certain companies to provide technical interfaces to enable government access. Other draft provisions would also require companies to share software source code and file encryption plans with the government. International concern has been conveyed to Chinese authorities, and it is not clear what impact this will have on future Chinese deliberations and drafts regarding these laws and potentially troubling provisions. The meeting in September 2015 between Presidents Xi Jinping and Barack Obama concluded with an agreement to collaborate on cybersecurity and efforts to crack down on cybercrime. They also jointly embraced a July 2015 United Nations accord to desist from targeting each other's critical infrastructure during peacetime. President Obama, however, spoke much more forcefully and specifically about stopping cyber-espionage used for commercial gain. The practical impacts of the September agreement between the two leaders remain to be seen, of course.

India also does not have comprehensive legislation directed towards data protection or cybersecurity. However, rules regarding 'reasonable security practices and procedures and sensitive personal data or information' have been issued under the Information Technology Act. These rules are intended to guide corporate practices. The rules call for companies to maintain privacy policies and transfer personal data outside India only to countries where there is an assurance of a level of protection equivalent to that provided by the company itself. Given the absence of a specific legislative mandate, however, there has been no significant litigation addressing corporate practices under these rules. Nonetheless, courts have been considering a constitutional right to privacy derived from the country's express guarantees for free expression and movement, and there is a common law right to privacy under India's tort regime.

In sum, the world is converging on more privacy laws that cover more areas of business and are subject to more enforcement. However, there are few efforts to harmonise the laws to promote interoperability and enhance digital trade and unfettered international data flows. The United States significantly leads the world in data protection enforcement, but many countries considering adopting new laws look to the EU model of omnibus and detailed regulation.

Fairly or otherwise, the ongoing impacts of the Snowden leaks still drive a wedge between the United States and the EU on privacy issues. 'Even' in the United States, however, it has been just about one year since the Chief Justice of the Supreme Court upheld the privacy of smartphone data that could have been useful to law enforcement because 'privacy comes at a cost'. For the private sector, prospective privacy constraints on big-data applications and other new technologies will also need to be looked at carefully so that the impacts on innovation, personalisation and consumer convenience are not unduly limited.

Given the increasing challenges of providing notice and obtaining consent with respect to data collection and use for ubiquitous connected technologies, new models for ethical data stewardship are likely to emerge soon. Indeed, in his Opinion of April 2015, 'Towards a New Digital Ethics', European Data Protection Supervisor (EDPS) Giovanni Buttarelli has proposed that an ethical framework needs to be at the foundation of the current digital ecosystem comprising big data, the internet of things, ambient computing, cloud and autonomous computing, artificial intelligence and many other new technologies. The EDPS considers that better respect for and safeguarding of human dignity would be at the heart of a new digital ethics.

By next year, privacy and cybersecurity developments will surely reveal whether the data protection paradigm has shifted to any significant degree, and whether businesses and the public continue to be able to develop and embrace technological innovation in socially useful ways that respect dignity as well as progress.

Chapter 2

EUROPEAN UNION OVERVIEW

William RM Long, Géraldine Scali and Alan Charles Raul[1]

I OVERVIEW

In the EU, data protection is principally governed by the EU Data Protection Directive 95/46/EC[2] (the Data Protection Directive), which regulates the collection and processing of personal data across all sectors of economy.

The Data Protection Directive has been implemented in all of the 28 EU Member States through national data protection laws. The reform of EU data protection laws has been the subject of intense discussion over the past couple of years with the European Commission publishing in January 2012 its proposal for an EU Data Protection Regulation,[3] which would replace the Data Protection Directive and introduce new data protection obligations for data controllers and processors and new rights for individuals. The proposal, which has now reached the final stages of negotiations, would also see significant new enforcement powers including fines of up to 5 per cent of annual worldwide turnover or €100 million, whichever is the greater.

Set out in this chapter is a summary of the main provisions in the Data Protection Directive and the proposed EU Data Protection Regulation. This chapter then covers

1 William RM Long and Alan Charles Raul are partners and Géraldine Scali is a senior associate at Sidley Austin LLP.

2 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation).

guidance provided by the EU's Article 29 Working Party on the topical issues of cloud computing and whistle-blowing hotlines. This chapter then concludes by considering the EU's proposed Network and Information Security Directive.

II EU DATA PROTECTION DIRECTIVE

The Data Protection Directive, as implemented into the national data protection laws of each Member State, imposes a number of obligations in relation to the processing of personal data. The Directive also provides several rights to data subjects in relation to the processing of their personal data.

Failure to comply with the Data Protection Directive, as implemented in the national laws of EU Member States, can amount to criminal offences and result in significant fines and civil claims from data subjects who have suffered as a result.

Although the Data Protection Directive sets out harmonised data protection standards and principles, the way it has been implemented by different Member States can vary significantly, with some requiring that the processing of personal data be notified to the local data protection authority (DPA).

i The scope of the Data Protection Directive

The Data Protection Directive is intended to apply to the processing of personal data wholly or partly by automatic means, and to the processing that forms part of a filing system. The Directive is not intended to apply to the processing of personal data by an individual in the course of a purely personal or household activity.

The Data Protection Directive, as implemented through national Member State law, only applies when the processing is carried out in the context of an establishment of the controller within the jurisdiction of a Member State, or alternatively, where the controller does not have an establishment in a Member State, processes personal data through equipment located in the Member State other than for the sole purpose of transit through that Member State. There are a number of important definitions used in the Directive, which include:[4]

a controller – any person who alone or jointly determines the purposes for which personal data is processed;

b data processor – a natural or legal person that processes personal data on behalf of the controller;

c data subject – an individual who is the subject of personal data;

d establishment – a controller that carries out the effective and real exercise of activity through stable arrangements in a Member State;[5]

e filing system – any structured set of personal data that is accessible according to specific criteria, whether centralised, or decentralised, such as a filing cabinet containing employee files organised according to their date of joining or their names;

4 Article 2 of the Data Protection Directive.

5 Recital 19 of the Data Protection Directive.

f personal data – data that relates to an individual who is identified or identifiable either directly or indirectly by reference to an identification number or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. In practice, this is a broad definition including anything from someone's name, address or national insurance number to information about their taste in clothes; and

g processing – any operation or set of operations performed upon personal data, such as collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This definition is so broad that it covers practically any activity in relation to personal data.

ii Obligations of controllers under the Data Protection Directive

Notification

Each Member State is obliged to set up a national DPA that controllers may be required to notify before commencing processing.[6] There are instances where some Member States can exempt controllers from this requirement. For example, if the controller has appointed a data protection officer who keeps an internal register of processing activities.[7]

Conditions for processing

Controllers may only process personal data if they have satisfied one of six conditions: (1) the data subject in question has consented to the processing; (2) the processing is necessary to enter into or perform a contract with the data subject; (3) the processing is necessary for the pursuit of a legitimate interest of the controller or a third party to whom the personal data are to be disclosed and the rights of the data subject not overridden; (4) the processing is necessary to comply with a legal obligation; (5) that the processing is necessary to protect the vital interests of the data subject; or (6) the processing is necessary for the administration of justice or carried out in fulfilment of a public interest function. Of these conditions the first three will be most relevant to business.[8]

Personal data that relates to a data subject's race or ethnicity, political life, trade union membership, religious or other similar beliefs, health or sex life (sensitive personal

6 Article 18 of the Data Protection Directive.

7 For example in Germany, the notification requirement does not apply: (1) if the data controller has appointed a data protection officer (Section 4d(2) of the Federal Data Protection Act); or (2) if the controller collects, processes or uses personal data for its own persons and no more than nine employees are employed in collecting, processing or using personal data, and either the data subject has given his or her consent or the collection, processing or use is needed to create, carry out or terminate a legal obligation or a quasi-legal obligation with the data (Section 4d(3) of the German Federal Data Protection Act).

8 Article 7 of the Data Protection Directive.

data) can only be processed in more narrowly defined circumstances.[9] The circumstances that will often be most relevant to a business would be where the data subject has explicitly consented to the processing.

Provision of information

Certain information needs to be provided by controllers to data subjects when controllers collect personal data about them, unless the data subjects already have that information. This information includes the identity of the controller (or the controller's representative), the purposes of the processing, and such further information as may be necessary to ensure that the processing is fair (e.g., the categories of personal data, the categories of recipients of the personal data and the existence of rights of data subjects to access and correct their personal data).[10] In instances where the personal data is not collected by the controller directly from the data subject concerned, the controller is expected to notify this information at the time it collects the personal data, or where a disclosure is envisaged, at the time the personal data is first disclosed. Also, in cases of indirect collection, it may be possible to avoid providing the required information if to do so would be impossible or involve a disproportionate effort, or if the collection is intended for scientific or historical research or is collection that is mandated by law.

Treatment of personal data

In addition to notification and providing information to data subjects as to how their personal data will be processed, controllers must ensure that the personal data they process is adequate, relevant and not excessive for the purposes for which they were collected. In addition controllers must keep the personal data accurate, up to date, and in a form that permits identification of the data subject for no longer than is necessary.[11]

Security

The controller will be responsible for ensuring that appropriate technical and organisational measures are in place to protect the personal data. A controller must also choose a data processor providing sufficient guarantees as to the security measures applied by the data processor. A controller must have a written contract with the data processor under which the data processor agrees to only process the personal data on the instructions of the controller, and that obliges the data processor to also ensure the same level of security measures as would be expected from the controller.[12]

9 Article 8 of the Data Protection Directive.

10 Article 10 of the Data Protection Directive.

11 Article 6 of the Data Protection Directive.

12 Article 17 of the Data Protection Directive.

Prohibition on transfers outside the EEA

Controllers may not transfer personal data to countries outside the European Economic Area (EEA)[13] unless the recipient country provides an adequate level of protection for the personal data.[14] The EU Commission can make a finding on the adequacy of any particular non-EEA state, and Member States are expected to give effect to such findings as necessary in their national laws. So far, the EU Commission has made findings of adequacy with respect to Andorra, Argentina, Australia, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. In addition, the United States has reached agreement with the EU Commission on a set of 'Safe Harbor' principles to which organisations in the United States may subscribe to be deemed 'adequate' to receive personal data from controllers in the EU.[15] However, this was in October 2015 declared invalid by the Court of Justice of the European Union (CJEU). The status of Safe Harbor version 2.0 is still unknown albeit negotiations between US authorities and the European Commission are ongoing.

Where transfers are to be made to countries that are not deemed adequate other exceptions may apply to permit the transfer.[16] These include where the data subject has unambiguously consented to the transfer, and where the transfer is necessary to perform or conclude a contract that the controller has with the data subject or, alternatively, with a third party if the contract is in the data subject's interests. In addition, the European Commission has approved the EU Model Contract Clauses, standard contractual clauses that may be used by controllers when transferring personal data to non-EEA countries (a model contract). There are two forms of model contract: one where both the data exporter and data importer are controllers; and another where the data exporter is a controller and the data importer is a data processor. Personal data transferred on the basis of a model contract will be presumed to be adequately protected. However, model contracts have been widely criticised as being onerous on the parties. This is because it grants third-party rights to data subjects to enforce the terms of the model contract against the data exporter and data importer, and requires the parties to the model contract to give broad warranties and indemnities. The clauses of the model contracts can also not be varied and model contracts can become impractical where there are a large number of data transfers that need to be covered by numerous model contracts.

An alternative means of authorising transfers of personal data outside the EEA is the use of binding corporate rules. This approach may be suitable for multinational companies transferring personal data within the same company, or within a group of companies. Under the binding corporate rules approach, the company would adopt a group-wide data protection policy that satisfies certain criteria, and if the rules bind the

13 The EEA consists of the 28 EU Member States together with Iceland, Liechtenstein and Norway.

14 Article 25 of the Data Protection Directive.

15 The US-EU Safe Harbor Framework was approved in 2000. Details of the Safe Harbor Agreement between the EU and the United States can be found in EU Commission Decision 520/2000/EC.

16 Article 26 of the Data Protection Directive.

whole group, then those rules could be approved by EU DPA as providing adequate data protection for transfers of personal data throughout the group. The Article 29 Working Party, which is composed of representatives of each Member State and advises the European Commission on data protection matters, has published various documents[17] on binding corporate rules including a model checklist for approval of binding corporate rules[18] with a table with the elements and principles to be found in binding corporate rules.[19]

iii Marketing

The EU Electronic Communications (Data Protection and Privacy) Directive 2002/58/EC (the ePrivacy Directive), places requirements on Member States in relation to the use of personal data for direct marketing. Direct marketing for these purposes includes unsolicited faxes, or making unsolicited telephone calls through the use of automated calling machines or direct marketing by email. In such instances the direct marketer needs to have the prior consent of the recipient (i.e., consent on an 'opt-in' basis). However, in the case of emails there are limited exceptions for email marketing to existing customers, where if certain conditions[20] are satisfied, unsolicited emails can still be sent without prior consent. In other instances of unsolicited communications it is left up to each Member State to decide whether such communications will require

17 WP 133 – Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data adopted on 10 January 2007.
WP 154 – Working Document setting up a framework for the structure of Binding Corporate Rules adopted on 24 June 2008.
WP 155 – Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules adopted on 24 June 2008 and last revised on 8 April 2009.
WP 195 – Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules adopted on 6 June 2012.
WP 195a – Recommendation 1/2012 on the standard application form for approval of Binding Corporate Rules for the transfer of personal data for processing activities adopted on 17 September 2012.
WP 204 – Explanatory document on the Processor Binding Corporate Rules last adopted on 22 May 2015.

18 WP 108 – Working Document establishing a model checklist application for approval of binding corporate rules adopted on 14 April 2005.

19 WP 153 – Working Document setting up a table with the elements and principles to be found in binding corporate rules adopted on 24 June 2008.

20 Unsolicited emails may be sent without prior consent to existing customers: (1) if the contact details of the customer have been obtained in the context of a sale of a product or a service and the unsolicited email is for similar products or services, and (2) if the customer has been given an opportunity to object free of charge in an easy manner to such use of his or her electronic contact details when they are collected and on the occasion of each message in the event the customer has not initially refused such use – Article 13 (2) of the ePrivacy Directive.

the recipient's prior consent or, alternatively can be sent without prior consent unless the recipient has indicated that they do not wish to receive such communications (i.e., consent on an 'opt-out' basis).

The ePrivacy Directive imposes requirements on providers of publicly available electronic communication services to put in place appropriate security measures and to notify certain security breaches in relation to personal data. The ePrivacy Directive has also been amended in 2009[21] to require that website operators obtain the informed consent of users to collect personal data of users through website 'cookies' or similar technologies used for storing information. There are two exemptions to the requirement to obtain consent before using cookies: (1) when the cookie is used for the sole purpose of carrying out the transmission of a communication over an electronic communications network; and (2) where the cookie is strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[22]

The Article 29 Working Party has published an opinion on the cookie consent exemption,[23] which provides an explanation on which cookies require the consent of website users (e.g., social plug-in tracking cookies, third-party advertising cookies used for behavioural advertising, analytics) and those which fall within the scope of the exemption (e.g., authentication cookies, multimedia player session cookies and cookies used to detect repeated failed login attempts). Guidance on how to obtain consent has been published at a national level by various data protection authorities.[24]

iv Rights of data subjects under the Data Protection Directive

Data subjects have a right to obtain access to personal data held about them and also to be able to ask for the personal data to be corrected where the personal data is inaccurate.[25]

Data subjects also have rights to object to certain types of processing where there are compelling legitimate grounds;[26] for example, where the processing would cause the data subject unwarranted harm. Data subjects may also object to direct marketing and to decisions that significantly affect them being made solely on the basis of automated processing.

In May 2014, the Court of Justice of the European Union issued a judgment against Google Inc and Google Spain SL in which it ruled that in certain circumstances search engines are obliged to remove links displayed following a search made on the basis of a person's name, where the data is incomplete or inaccurate, even if the publication itself on those web pages is lawful. This is based on existing rights under the EU Data Protection Directive to rectification, erasure or blocking of personal data where the

21 Directive 2009/56/EC.

22 Article 5(3) of the ePrivacy Directive.

23 WP 194 – Opinion 04/2012 on Cookie Consent Exemption.

24 For example: UK Information Commissioner's Office 'Guidance on the rules on use of cookies and similar technologies'; and the French Commission National de l'informatique et des libertés.

25 Article 12 of the Data Protection Directive.

26 Article 14 of the Data Protection Directive.

individual objects to the processing of such data for compelling legitimate grounds, where the data is inadequate, irrelevant or inaccurate, or excessive in relation to the purposes of the processing, and where the impact on an individual's privacy is greater than the public's right to find the data. As at May 2015 Google had received over 253,000 removal requests and had removed approximately 380,000 links from search results.

III PROPOSED EU DATA PROTECTION REGULATION

As referred to above, the current EU data protection regime is subject to review with intensive discussion on the proposed EU Data Protection Regulation (the Regulation). The Regulation was published by the European Commission in January 2012 and has been described as the most lobbied piece of European legislation in history, receiving over 4,000 amendments in opinions from committees in the European Parliament as well as from numerous industries. In March 2014 the European Parliament's Civil Liberties Committee after several delays finally voted on the European Commission's proposed EU Data Protection Regulation and adopted all amendments. Over a year later, in June 2015, the Council of Ministers (which represents EU Member States) published its compromise proposal for the Regulation. This in turn, triggered the commencement of the 'trilogue' process – the final stage of negotiations between the three EU institutions. It is thought that adoption of the Regulation may occur by the end of 2015 or early 2016.

The proposed Regulation once adopted will have a significant impact on many governments, businesses and individuals both in the EU and outside the EU. The main elements of the proposed Regulation are summarised below.

i Enforcement

As proposed by the European Parliament, the amount of the maximum fines for non-compliance with the proposed Regulation is 5 per cent of annual worldwide turnover or €100 million, whichever is the greater, with an ability for individuals to bring claims for non-compliance. The European Commission and the Council of Ministers both proposed slightly lower but no less significant fines of 2 per cent of annual worldwide turnover or €1 million, whichever is the greater. While the Parliament's draft allowed for any association acting in the public interest to bring claims for non-compliance, the Council's draft limited this to statutory bodies that aim to protect the interests of individuals and only where acting on the instructions of an individual.

ii Scope of the Regulation

The Regulation will apply to the processing of personal data in the context of the activities of a data controller or a processor in the EU and to a controller or processor not established in the EU, where the processing activities are related to: (1) the offering of goods or services to EU citizens; or (2) the monitoring of such individuals. This means that many non-EU companies that have EU customers will need to comply with the proposed Regulation once implemented.

iii One-stop shop

The Regulation proposes a new regulatory 'one-stop shop' for data controllers that operate in several EU countries. The DPA where the controller is established will be the lead DPA, which must consult with other DPAs before taking action. In the case of a dispute between DPAs, action can be decided upon by the European Data Protection Board. As proposed by the Council, the lead DPA must reach a consensus on any decision with all DPAs concerned.

iv Profiling

Significantly for online companies, under the Regulation, every individual will now have a general right to object to profiling. In addition, the Regulation imposes a new requirement to inform individuals about the right to object to profiling in a 'highly visible manner'. Profiling that significantly affects the interests of an individual can only be carried out under limited circumstances, such as with the individual's consent and should not be automated, but involve human assessment. These provisions if adopted could have a major impact on how online companies market their products and services.

v Explicit consent

As proposed by the Commission and the Parliament, consent for processing personal data should be explicit, with affirmative action required under the proposed Regulation. The mere use of a service will not amount to consent. The Council's draft only requires consent to be explicit where processing sensitive personal data. According to the Regulation, it should also be as easy to withdraw consent as it is to give it, with consent being invalid where given for unspecified data processing. Processing data on children under 13 also requires the consent of the parent or legal guardian. Companies also cannot make the execution of a contract or a provision of a service conditional upon the receipt of consent from users to process their data.

vi Standardised information policies

The proposal from the Parliament requires that certain standardised information should be provided to individuals in the form of symbols or icons similar to those used in the food industry. All proposed texts agree that individuals should be informed about how their personal data will be processed and their rights of access to data, rectification and erasure of data and of the right to object to profiling as well as to lodge a complaint with a DPA and to bring legal proceedings.

vii Right of erasure

The 'right of erasure' (formerly the 'right to be forgotten') gives individuals a right to have their personal data erased where the data is no longer necessary or where they withdraw consent, although a limited number of exemptions also apply, such as where data is required for scientific research or for compliance with a legal obligation of EU law.

viii Accountability

Controllers will be required to adopt all reasonable steps to implement compliance procedures and policies that respect the choices of individuals, which should be reviewed every two years. Importantly, controllers will need to implement privacy by design throughout the life cycle of processing from collection of the data to its deletion. In addition, businesses will need to keep detailed documentation of the data being processed and carry out a privacy impact assessment where the processing presents specific risks, such as the use of health data or where the data involves more than 5,000 individuals. This assessment also has to be reviewed every two years.

ix Data protection officers

According to the Parliament, businesses that process data on more than 5,000 people in any 12-month period, or that process sensitive data such as health data, should appoint a data protection officer, who should have extensive knowledge of data protection and who does not necessarily need to be an employee. The Commission requires such an appointment to be made where the business has more than 250 employees. However, under the Council's proposal the appointment is voluntary unless otherwise compulsory under national Member State law.

x Security and security breaches

The controller and the processor will need to implement appropriate technical and organisational security measures. The proposal also requires that security policies contain a number of elements including, for example, a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness. In addition, security breaches will need to be notified to DPAs and affected individuals without undue delay.

xi International data transfers

In addition to binding corporate rules and other data transfer solutions, new methods allowing for international data transfers of personal data from the EU include the use of approved codes of conduct or certification mechanisms. The Council's proposal also permits such transfers where they are necessary for the 'legitimate interests' of the controller, providing such transfers are not large scale or frequent, the controller has adduced appropriate safeguards and the interests of the affected individuals are not overridden. Parliament's proposal also reintroduced an important provision requiring that any requests for access to personal data by foreign authorities or courts outside the EU must be authorised by a DPA.

xii Health data

The Regulation also has important provisions relating to the use of health data including the processing of personal data for scientific research, which, according to the Parliament's proposal, is only permitted where it is not otherwise possible to use anonymous or pseudonymous data under the highest technical standards with measures

to prevent re-identification of individuals. However, as proposed by the Council, the scientific research must be conducted in accordance with Member State laws, subject always to the implementation of appropriate safeguards.

IV CLOUD COMPUTING

In its guidance on Cloud Computing adopted on 1 July 2012,[27] the EU's Article 29 Working Party states that the majority of data protection risks can be divided into two main categories: (1) the lack of control over the data; and (2) insufficient information regarding the processing operation itself. The lawfulness of the processing of personal data in the cloud depends on the adherence to principles of the EU Data Protection Directive, which are considered in the Article 29 Working Party Opinion and some of which are summarised below.

i Instructions of the data controller

To comply with the requirements of the EU Data Protection Directive the Article 29 Working Party Opinion provides that the extent of the instructions should be detailed in the relevant cloud computing agreement (the agreement) along with service levels and financial penalties on the provider for non-compliance.

ii Purpose specification and limitation requirement[28]

Under Article 6(b) of the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. To address this requirement, the agreement between the cloud provider and the client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or the subcontractors.

iii Security[29]

Under the Data Protection Directive, the data controller must have in place adequate organisational and technical security measures to protect personal data and should be able to demonstrate accountability. The Article 29 Working Party Opinion comments on this point, reiterating that it is of great importance that concrete technical and organisational measures are specified in the cloud agreement, such as availability, confidentiality, integrity, isolation, and portability. As a consequence, the agreement with the cloud provider should contain a provision to ensure that the cloud provider and its subcontractors comply with the security measures imposed by the client. It should also contain a section regarding the assessment of the security measures of the cloud provider.

27 WP 196 – Opinion 5/2012 on Cloud Computing.

28 Article 6(b) of the Data Protection Directive.

29 Article 17(2) of the Data Protection Directive.

The agreement should also contain an obligation for the cloud provider to inform the client of any security event. The client should also be able to assess the security measures put in place by the cloud provider.

iv Subcontractors

The Article 29 Working Party Opinion indicates that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the agreement. There should also be a clear obligation on the cloud provider to name all the subcontractors commissioned, as well as the location of all data centres where the client's data can be hosted. It must also be guaranteed that both the cloud provider and all the subcontractors shall act only on instructions from the client. The agreement should also set out the obligation on the part of the processor to deal with international transfers, for example by signing contracts with sub-processors, based on the EU Model Contract Clauses.

v Erasure of data[30]

The Article 29 Working Party Opinion states that specifications on the conditions for returning the personal data or destroying the data once the service is concluded should be contained in the agreement. It also states that data processors must ensure that personal data is erased securely at the request of the client.

vi Data subject rights[31]

According to the Article 29 Working Party Opinion, the agreement should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subject's rights to access, correct or delete their and to ensure that the same holds true for the relation to any subcontractor.

vii International transfers[32]

As discussed above, under Articles 25 and 26 of the Data Protection Directive, personal data can only be transferred to countries located outside the EEA if the country provides an adequate level of protection.

viii Confidentiality

The Article 29 Working Party Opinion recommends that an agreement with the cloud provider should contain confidentiality wording that is binding both upon the cloud provider and any of its employees who may be able to access the data.

30 Article 6 (e) of Data Protection Directive.

31 Article 12 and 14 of the Data Protection Directive.

32 Article 25 and 26 of the Data Protection Directive.

ix Request for disclosure of personal data by a law enforcement authority

Under the Article 29 Working Party Opinion, the client should be notified about any legally binding request for disclosure of the personal data by law enforcement authority unless otherwise prohibited, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

x Changes concerning the cloud services

The Article 29 Working Party recommends that the agreement with the cloud provider should contain a provision stating that the cloud provider must inform the client about relevant changes concerning the respective cloud service, such as the implementation of additional functions.

V WHISTLE-BLOWING HOTLINES

The Article 29 Working Party published an opinion in 2006 on the application of the EU data protection rules to whistle-blowing hotlines[33] providing various recommendations, which are summarised below.

i Legitimacy of whistle-blowing schemes

Under the Data Protection Directive personal data must be processed fairly and lawfully. For a whistle-blowing scheme this means that the processing of personal data must be on the basis of at least one of certain grounds, the most relevant of which include where:

a the processing is necessary for compliance with a legal obligation to which the data controller is subject, which could arguably include a company's obligation to comply with the provisions of the US Sarbanes-Oxley Act (SOX). However, the Article 29 Working Party concluded that an obligation imposed by a foreign statute, such as SOX, does not qualify as a legal obligation that would legitimise the data processing in the EU; or

b the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests or the fundamental rights and freedoms of the data subject. The Article 29 Working Party acknowledged that whistle-blowing schemes adopted to ensure the stability of financial markets and in particular the prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting as well as the fight against bribery, banking and financial crime, or insider trading might be seen as serving a legitimate interest of a company that would justify the processing of personal data by means of such schemes.

33 WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

ii Limiting the number of persons eligible for using the hotline

Applying the proportionality principle, the Article 29 Working Party recommends that the company responsible for the whistle-blowing reporting programme, should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct and the number of persons who might be incriminated. However, the recommendations acknowledged that in both cases the categories of personnel involved may still sometimes include all employees in the fields of accounting, auditing and financial services.

iii Promotion of identified reports

The Article 29 Working Party pointed out that although in many cases anonymous reporting is a desirable option, where possible, whistle-blowing schemes should be designed in such a way that do not encourage anonymous reporting. Rather, the helpline should obtain the contact details of reports, and maintain the confidentiality of that information within the company, for those who have a specific need to know the relevant information. The Article 29 Working Party also suggested that only reports that included identifiable information from the whistle-blower would be considered a 'fairly' collected report.

iv Proportionality and accuracy of data collected

Companies should clearly define the type of information to be disclosed through the system by limiting the information to accounting, internal accounting control or auditing or banking and financial crime and anti-bribery. The personal data should be limited to data strictly and objectively necessary to verify the allegations made. In addition, complaint reports should be kept separate from other personal data.

v Compliance with data-retention periods

According to the Article 29 Working Party, personal data processed by a whistle-blowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report. Such periods would be different when legal proceedings or disciplinary measures are initiated. In such cases, personal data should be kept until the conclusion of these proceedings and the period allowed for any appeal. Personal data found to be unsubstantiated should be deleted without delay.

vi Provision of clear and complete information about the whistle-blowing programme

Companies as data controllers must provide information to employees about the existence, purpose and operation of the whistle-blowing programme, the recipients of the reports, and the right of access, rectification and erasure for reported persons. Users should also be informed that the identity of the whistle-blower shall be kept confidential, that abuse of the system may result in action against the perpetrator of that abuse, and that they will not face any sanctions if they use the system in good faith.

vii Rights of the incriminated person

The Article 29 Working Party noted that it was essential to balance the rights of the incriminated person, the whistle-blower, and the company's legitimate investigative needs. In accordance with the Data Protection Directive, an accused person should be informed by the person in charge of the ethics reporting programme as soon as practicably possible after the ethics report implicating them is received. The implicated employee should be informed about: the entity responsible for the ethics reporting programme; the acts of which he or she is accused; the departments or services that might receive the report within the company or in other entities or companies of the corporate group; and how to exercise his or her rights of access and rectification.

Where there is a substantial risk that such notification would jeopardise the ability of the company to effectively investigate the allegation or gather evidence, then notification to the incriminated person may be delayed as long as such risk exists.

The whistle-blowing scheme also needs to ensure compliance with the individual's right, under the Data Protection Directive, of access to personal data on them and their right to rectify incorrect, incomplete or outdated data. However, the exercise of these rights may be restricted to protect the rights of others involved in the scheme and under no circumstances can the accused person obtain information about the identity of the whistle-blower, except where the whistle-blower maliciously makes a false statement.

viii Security

The company responsible for the whistle-blowing scheme must take all reasonable technical and organisational precautions to preserve the security of the data and to protect against accidental or unlawful destruction or accidental loss and unauthorised disclosure or access. Where the whistle-blowing scheme is run by an external service provider the EU data controller needs to have in place a data processing agreement and must take all appropriate measures to guarantee the security of the information processed throughout the whole process and commit themselves to complying with the data protection principles.

ix Management of whistle-blowing hotlines

A whistle-blowing scheme needs to carefully consider how reports are to be collected and handled with a specific organisation set up to handle the whistle-blower's reports and lead the investigation. This organisation must be composed of specifically trained and dedicated people, limited in number and contractually bound by specific confidentiality obligations. The whistle-blowing system should be strictly separated from other departments of the company, such as human resources.

x Data transfers from the EEA

The Working Party believes that groups should deal with reports locally in one EEA state rather than automatically share all the information with other group companies. However, data may be communicated within the group if such communication is necessary for the investigation, depending on the nature or seriousness of the reported misconduct or results from how the group is set up. Such communication will be considered necessary, for example, if the report incriminates another legal entity within

the group involving a high-level member of management of the company concerned. In this case, data must only be communicated under confidential and secure conditions to the competent organisation of the recipient entity, which provides equivalent guarantees as regards management of the whistle-blowing reports as the EU organisation.

VI E-DISCOVERY

The Article 29 Working Party has published a Working Document providing guidance to data controllers in dealing with requests to transfer personal data to other jurisdiction outside the EEA for use in civil litigation[34] to help them to reconcile the demands of a litigation process in a foreign jurisdiction with the data protection obligations of the Data Protection Directive.

The main suggestions and guidelines include the following:

a Possible legal bases for processing personal data as part of a pretrial e-discovery procedure include consent of the data subject and compliance with a legal obligation. However, the Article 29 Working Party states that an obligation imposed by a foreign statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. A third possible basis is a legitimate interest pursued by the data controller or by the third party to whom the data is disclosed where the legitimate interests are not overridden by the fundamental rights and freedoms of the data subjects. This involves a balance-of-interest test taking into account issues of proportionality, the relevance of the personal data to litigation and the consequences for the data subject.

b Restricting the disclosure of data if possible to anonymised or redacted data as an initial step and after culling the irrelevant data, disclosing a limited set of personal data as a second step.

c Notifying individuals in advance of the possible use of their data for litigation purposes and, where the personal data is actually processed for litigation, notifying the data subject of the identity of the recipients, the purposes of the processing, the categories of data concerned and the existence of their rights.

d Where the non-EEA country to which the data will be sent does not provide an adequate level of data protection and where the transfer is likely to be a single transfer of all relevant information then there would be a possible ground that the transfer is necessary for the establishment, exercise or defence of a legal claim. Where a significant amount of data is to be transferred, the Article 29 Working Party previously suggested the use of binding corporate rules or the Safe Harbor regime. However, Safe Harbor was recently found to be invalid by the CJEU. It also recognises that compliance with a request made under the Hague Convention would provide a formal basis for the transfer of the data.

34 WP 158 – Working Document 1/2009 on pretrial discovery for cross-border civil litigation adopted on 11 February 2009.

VII EU CYBERSECURITY STRATEGY

In March 2014 the European Parliament adopted a proposal for a Network and Information Security Directive[35] (the NIS Directive), which had been proposed by the European Commission in 2013. The NIS Directive is part of the European Union's Cyber Security Strategy aimed at tackling network and information security incidents and risks across the EU.

The main elements of the proposed NIS Directive include a new national strategy, a cooperation network and certain security requirements.

i New national strategy

The NIS Directive requires Member States to adopt a national strategy setting out concrete policy and regulatory measures to maintain a level of network and information security.[36] This includes designating a competent national authority for information security and the setting up of a computer emergency response team that is responsible for handling incidents and risks.

ii Cooperation network

The competent authorities in EU Member States and the European Commission will form a cooperation network to coordinate against risks and incidents affecting network and information systems.[37] The cooperation network will exchange information between authorities and also provide early warnings on information security risks and incidents and agree on a co-ordinated response in accordance with an EU NIS cyber-cooperation plan.

iii Security requirements

A key element of the NIS Directive is that Member States must ensure public bodies and certain market operators[38] take appropriate technical and organisational measures to manage the security risks to networks and information systems and to guarantee a level of security appropriate to the risks.[39] The measures should prevent and minimise the impact

35 Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 7 February 2013.

36 Article 5 of the proposed NIS Directive.

37 Article 8 of the proposed NIS Directive.

38 Market operators are listed in Annex II of the NIS Directive as amended by the European Parliament and includes operators in energy and transport, financial market infrastructures, operators in the water production and supply and the food supply chain and internet exchange points. It should be noted that information service providers (e.g., e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and application stores) were included in the European Commission's proposal, but it was provisionally agreed in June 2015 that information service providers would not be required to comply in full with the proposed NIS Directive.

39 Article 14 of the proposed NIS Directive.

of security incidents affecting the core services they provide. Public bodies and market operators must also notify the competent authority of incidents having a significant impact on the continuity of the core services they provide and the competent authority may decide to inform the public of the incident. According to amendments by the European Parliament the significance of the incident should take into account: (1) the number of users affected; (2) the duration of the incident; and (3) the geographic spread of the area affected by the incident.

The NIS Directive will now need to be agreed with the EU's Council of Ministers and may be adopted in 2016.

VIII OUTLOOK

The final stages of negotiations in respect of the proposed EU Data Protection Regulation are under way, with EU legislators determined to reconcile any differences and reach an agreement by the end of 2015 or early 2016. It is important, therefore, that businesses in all industries start to consider how to comply with the new requirements under the proposed Regulation.

In June 2015 the European Data Protection Supervisor (EDPS) published its draft text of the proposed EU Data Protection Regulation. The EDPS took a less prescriptive approach than the other EU legislators, stating that details on compliance should come via guidance from the European Data Protection Board. This resulted in a text 30 per cent shorter than any of the other proposals. Overall the text proposed by the EDPS backed the proposal from the European Parliament including in relation to proposed fines and timings in which to notify data security breaches. The EDPS released at the same time a mobile app that compares the four texts alongside one another.

In 2015 the Article 29 Working Party published its report on the cookie sweep it undertook in 2014. The sweep was carried out by the Article 29 Working Party together with eight DPAs and covered 478 websites across three sectors. The sweep was an information-gathering exercise to better understand the level of compliance with the ePrivacy Directive.[40] It consisted of both an automated statistical review of the cookies used and a manual review of the information and consent mechanisms used. Key findings included the following information: of the 478 websites reviewed only seven did not set cookies; over 86 per cent of cookies were persistent cookies (i.e., cookies that remain on a user's device beyond the closing of the browser); the most common notification method used was a cookie banner; and 26 per cent of the websites reviewed failed to show any cookie notification on the landing page. What actions will be taken in response to these results are not known.

On 6 October 2015 the CJEU issued its ruling[41] in the closely watched *Max Schrems* case challenging the US-EU Safe Harbor Agreement, finding the European

40 ePrivacy Directive 2002/58/EC, as amended by 2009/136/EC.

41 Available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb056ace3a8b4ceab1408435ca66794e.e34KaxiLc3eQc40LaxqMbN4Oc30Se0?text=&docid=169195&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=205995.

Commission's decision on Safe Harbor to be invalid. As predicted by many, the ruling follows the opinion[42] of Advocate General Yves Bot at the CJEU published on 23 September 2015.

The *Max Schrems* case concerns the Irish Data Protection Commissioner's decision not to investigate a complaint made by Schrems regarding the storage by Facebook of its EU subscribers' data on servers in the United States. More broadly, the case questions the adequacy of the US-EU Safe Harbor scheme. The reasons given by the CJEU in declaring Safe Harbor invalid include the ability of Safe Harbor-certified companies to disregard the Safe Harbor Principles where they conflict with national security, public interest and law enforcement requirements, and the inability of EU citizens to obtain legal redress where data is transferred to the United States.

In a press conference following the publication of the CJEU judgment, the Commission confirmed that it was going to step up ongoing talks with US authorities with regard to Safe Harbor version 2.0 and work with the Article 29 Working Party to issue guidance to national DPAs to ensure a coordinated response to alternative data transfer solutions. Preliminary guidance was issued by the Working Party on 16 October 2015, in which it was confirmed that: (1) enforcement action from DPAs against companies failing to implement appropriate data transfer solutions would not commence until after January 2016; (2) Safe Harbor version 2.0 is still a possibility providing this contains 'obligations on the necessary oversight of access by public authorities, on transparency, on proportionality, on redress mechanisms and on data protection rights'; and (3) EU Model Contract Clauses and binding corporate rules are still currently effective data transfer solutions. Businesses that relied on Safe Harbor to legitimise transfers of personal data from the EU to the United States prior to 6 October 2015 will have until the end of January 2016 to reconsider their choice of international data transfer solutions, and consider whether to adopt alternative solutions, such as binding corporate rules or EU Model Contract Clauses.

42 Available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd5a04f0a61298439ca282c192cebd5705.e34KaxiLc3qMb40Rch0SaxuRaN90?text=&docid=168421&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=438244.

Chapter 3

APEC OVERVIEW

Catherine Valerio Barrad and Alan Charles Raul[1]

I OVERVIEW

Asia-Pacific Economic Cooperation (APEC) is an organisation of economic entities in the Asia-Pacific region formed to enhance economic growth and prosperity in the region. It was established in 1989 by 12 Asia-Pacific economies as an informal ministerial-level dialogue group. Because APEC is primarily concerned with trade and economic issues, the criterion for membership is an economic entity rather than a nation. For this reason, its members are usually described as 'APEC member economies' or 'APEC economies'. Since 1993, the heads of the member economies have met annually at an APEC Economic Leaders Meeting, which has since grown to include 21 member economies as of August 2015: Australia, Brunei, Canada, Chile, China, Hong Kong, Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Taiwan, Thailand, the United States, and Vietnam.[2] Collectively, the 21 member economies account for more than half of world real GDP in purchasing power parity and over 44 per cent of total world trade.[3]

The main aim of APEC is to fulfil the goals established in 1994 at the Economic Leaders Meeting in Bogor, Indonesia of free and open trade and investment in the Asia-Pacific area for both industrialised and developing economies. APEC established a framework of key areas of cooperation to facilitate achievement of these 'Bogor Goals'. These areas, also known as the three pillars of APEC, are the liberalisation of trade and investment, business facilitation, and economic and technical cooperation. In recognition of the exponential growth and transformative nature of electronic

1 Catherine Valerio Barrad and Alan Charles Raul are partners at Sidley Austin LLP.

2 The current list of APEC member economies can be found at: www.apec.org/About-Us/About-APEC/Member-Economies.aspx.

3 See http://statistics.apec.org/.

commerce, and its contribution to economic growth in the region, APEC established an Electronic Commerce Steering Group (ECSG) in 1999, which began to work toward the development of consistent legal, regulatory and policy environments in the Asia-Pacific area.[4] It further established the Data Privacy Subgroup under the ECSG in 2003 to address privacy and other issues identified in the 1998 APEC Blueprint for Action on Economic Commerce.[5]

Because of varied domestic privacy laws among the member economies (including economies at different stages of legislative recognition of privacy), APEC concluded that a regional agreement that creates a minimum privacy standard would be the optimal mechanism for facilitating the free flow of data among the member economies (and thus promoting electronic commerce). The result was the principles-based APEC Privacy Framework, which was endorsed by the APEC economies in 2004. Although consistent with the original OECD Guidelines, the APEC Privacy Framework also provided assistance to member economies in developing data privacy approaches that would optimise the balance between privacy protection and cross-border data flows.

Unlike other privacy frameworks, APEC does not impose treaty obligation requirements on its member economies. Instead, the cooperative process among APEC economies relies on non-binding commitments, open dialogue and consensus. Member economies undertake commitments on a voluntary basis. Consistent with this approach, the APEC Privacy Framework is advisory only, and thus has few legal requirements or constraints.

APEC recently developed the Cross-Border Privacy Rules (CBPR) system, under which companies trading within the member economies develop their own internal business rules consistent with the APEC privacy principles to secure cross-border data privacy. In 2015, APEC developed the Privacy Recognition for Processors (PRP) system, a corollary to the CBPR system for data processors. APEC is also working with the EU to study potential interoperability of the APEC and EU data privacy regimes, and in 2014 issued a joint referential document that maps the requirements of the two regimes for the benefit of businesses that seek certification or approval under both systems. A common questionnaire, and a referential document for processors, are also under development.

The APEC Privacy Framework, the CBPR and PRP systems, the cooperative privacy enforcement system, and the 'APEC–EU Referential' are all described in more detail below.

---

4 The ECSG was originally established as an APEC senior officials' special task force, but in 2007 was realigned to the Committee on Trade and Investment. This realignment underscores the focus within the ECSG, and its Data Privacy Subgroup, on trade and investment issues.

5 APEC endorsed the Blueprint in 1998 to 'develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy […] and consumer protection'. See APEC Privacy Framework, at 2 (available at: www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx).

II APEC PRIVACY FRAMEWORK

i Introduction

The APEC Privacy Framework was developed to promote a consistent approach to information privacy protection in the Asia-Pacific region as a means of ensuring the free flow of information in support of economic development. It was an outgrowth of the 1998 APEC Blueprint for Action on Electronic Commerce, which recognised that the APEC member economies needed to develop and implement legal and regulatory structures to build public confidence in the safety and security of electronic data flows (including consumers' personal data) to realise the potential of electronic commerce. This recognition was the impetus behind the development of the Privacy Framework. Thus, the APEC objective of protecting informational privacy arises in the context of promoting trade and investment, rather than primarily to protect basic human rights as in the European Union.

The APEC Privacy Framework represents a consensus among economies with different legal systems, cultures and values, and that at the time of endorsement were at different stages of adoption of domestic privacy laws and regulations. Thus, the Framework provided a basis for the APEC member economies to acknowledge and implement basic principles of privacy protection, while still permitting for variation among them. It further provides a common basis on which to address privacy issues in the context of economic growth and development, both among the member economies, and between them and other trading entities.

ii The Privacy Framework

The Privacy Framework has four parts. Part I is a preamble that sets out the objectives of the principles-based Framework and discusses the basis on which consensus was reached; Part II describes the scope of the Privacy Framework and the extent of its coverage; Part III sets out the information privacy principles, including an explanatory commentary on them; and Part IV discusses implementation of the Privacy Framework, including providing guidance to member economies on options for domestic implementation.

Objectives and scope of the Privacy Framework (Parts I and II)

The market-oriented approach to data protection is reflected in the objectives of the Privacy Framework, which include – in addition to the protection of information – the prevention of unnecessary barriers to information flows, the promotion of uniform approaches by multinational businesses to the collection and use of data, and the facilitation of domestic and international efforts to promote and enforce information privacy protections. The Framework was designed for broad-based acceptance across member economies by encouraging compatibility while still respecting the different cultural, social and economic requirements within the economies. As such, the Framework sets an advisory minimum standard, and permits member economies to adopt stronger, and country-specific data protection laws.

The Privacy Framework cautions that the principles should be interpreted as a whole, rather than individually, because they are interconnected, particularly in how they balance privacy rights and the market-oriented public interest. These principles are

not intended to impede governmental activities within the member economies that are authorised by law, and thus the principles allow exceptions that will be consistent with particular domestic circumstances.[6] The Framework specifically recognises that there 'should be flexibility in implementing these Principles'.[7]

The nine principles of the Privacy Framework (Part III)

Given that seven of the original APEC member economies were members of the OECD, it is not surprising that the APEC Privacy Framework was based on the original OECD Guidelines. The APEC privacy principles address personal information about living individuals, and exclude both publicly available information and information connected with domestic affairs. The principles apply to persons or organisations in both public and private sectors who control the collection, holding, processing or use of personal information. Organisations that act as agents for others are excluded from compliance.

While based on the OECD Guidelines, the APEC principles are not identical to them. Missing are the OECD Guidelines of 'purpose specification' and 'openness', although aspects of these can be found within the nine principles – for example, purpose limitations are incorporated in Principle 4 regarding use of information. The APEC principles also permit a broader scope of exceptions and are slightly stronger than the OECD Guidelines on notice. In general, the APEC principles reflect the objective of promoting economic development and the respect for differing legal and social values among the member economies.

Principle I – Preventing Harm

This principle provides that privacy protections be designed to prevent harm to individuals from wrongful collection or misuse of their personal information, and that remedies for infringement be proportionate to the likelihood and severity of harm.

Principle II – Notice

The notice principle addresses the information that a data controller must include in a notice to individuals when collecting their personal information. It also requires that all reasonable steps be taken to provide the notice either before or at the time of collection, and if not, then as soon after collection as is reasonably practicable. The principle further provides for an exception for notice of collection and use of publicly available information.

Principle III – Collection Limitation

This principle provides for the lawful and fair collection of personal information limited to that which is relevant to the purpose of collection and, where appropriate, with notice to, or consent of, the data subject.

6 See APEC Privacy Framework, paragraph 13.

7 See APEC Privacy Framework, paragraph 12.

Principle IV – Uses of Personal Information
This principle limits the use of personal information to those uses that fulfil the purpose of collection and other compatible or related purposes. It includes exceptions for information collected with the consent of the data subject, collection necessary to complete a request of the data subject, or as required by law.

Principle V – Choice
The choice principle directs that, where appropriate, individuals be provided with mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information, with an exception for publicly available information. This principle also contemplates that, in some instances, consent can be implied or is not necessary.

Principle VI – Integrity of Personal Information
This principle states that personal information should be accurate, complete, and maintained up-to-date to the extent necessary for the purpose of use.

Principle VII – Security Safeguards
This principle requires that security safeguards be applied to personal data that are appropriate and proportional to the likelihood and severity of threatened harm, the sensitivity of the data and the context in which it is held, and that such safeguards be periodically reassessed.

Principle VIII – Access and Correction
The access and correction principle directs that individuals have the right of access to their personal information within a reasonable time and in a reasonable manner, and may challenge its accuracy and request appropriate correction. This principle includes exceptions when the burden of access or correction outweighs the risks to individual privacy, the information is subject to legal or security holds, or where privacy rights of other data subjects may be affected.

Principle IX – Accountability
This principle requires that a data controller be accountable for complying with measures that give effect to the nine principles and that, when transferring personal information, it should take reasonable steps to ensure that the recipients also protect the information in a manner that is consistent with the principles. This has often been described as the most important innovation in the APEC Privacy Framework, and it has been influential in encouraging other privacy regulators to consider similar accountability processes tailored to the risks associated with that specific data.

Unlike other international frameworks, the APEC Privacy Framework neither restricts the transfer of data to countries without APEC-compliant data protection laws nor requires such a transfer to countries with APEC-compliant laws. Instead, APEC adopted the accountability principle in lieu of data import and export limitations as being more consistent with modern business practices and the stated objectives of the Framework.

Implementation (Part IV)

Because APEC is a cooperative organisation, the member economies are not required to convert the Privacy Framework into domestic legislation. Rather, the Privacy Framework encourages the member economies to implement it without requiring or proposing any particular means of doing so. It suggests that there are 'several options for giving effect to the Framework […] including legislative, administrative, industry self-regulatory or a combination of these methods'.[8] The Framework advocates 'an appropriate array of remedies […] commensurate with the extent of the actual or potential harm' and supports a choice of remedies appropriate to each member economy. The Privacy Framework does not contemplate a central enforcement entity.

Thus, the APEC Privacy Framework contemplates variances in implementation across member economies. It encourages member economies to share information, surveys and research, and to engage in cross-border cooperation in investigation and enforcement.[9] This concept later developed into the Cross-Border Privacy Enforcement Arrangement (CPEA – see Section III.iii, *infra*).

iii Data privacy individual action plans

Data privacy individual action plans (IAPs) are periodic, national reports to APEC on each member economy's progress of adopting the Privacy Framework domestically. IAPs are the mechanism of accountability by member economies to each other for implementation of the APEC Privacy Framework.[10] The IAPs are periodically updated as the Privacy Framework is implemented within each such economy. As of 2015, 14 member economies have posted IAPs on the APEC website.[11]

III APEC CROSS-BORDER DATA TRANSFER

i Data Privacy Pathfinder initiative

The APEC Privacy Framework does not explicitly address the issue of cross-border data transfer, but rather calls for cooperative development of cross-border privacy rules.[12] In 2007, the APEC ministers endorsed the APEC Data Privacy Pathfinder initiative with the goal of achieving accountable cross-border flow of personal information within the Asia-Pacific region. The Data Privacy Pathfinder initiative contains general commitments leading to the development of an APEC CBPR system that would support accountable cross-border data flows consistent with the APEC Privacy Principles.

The main objectives of the Pathfinder initiative are to promote a conceptual framework of principles for the execution of cross-border privacy rules across APEC economies, to develop consultative processes among the stakeholders in APEC member

8 See APEC Privacy Framework, paragraph 31.

9 See APEC Privacy Framework, paragraphs 40–45.

10 See APEC Privacy Framework, paragraph 39.

11 See: www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx.

12 See APEC Privacy Framework, paragraphs 46–48.

economies for the development of implementing procedures and documents supporting cross-border privacy rules, and to implement an accountable cross-border privacy system. Since 2008, the Data Privacy Subgroup has been working on nine interrelated projects to support the development of cross-border privacy rules in the Asia-Pacific region. Both the CBPR system and the CPEA are outcomes of the Pathfinder initiative.

ii The CBPR system

The APEC CBPR system, endorsed in 2011, is a voluntary accountability-based system governing electronic flows of private data among APEC economies. As a newly established system, the CBPR system is in early stages of implementation. As of August 2015, four APEC economies participate in the CBPR system – Canada, Japan, Mexico and the United States – with more expected to join).

In general, the CBPR system requires businesses to develop their own internal privacy-based rules governing the transfer of personal data across borders under standards that meet or exceed the APEC Privacy Framework. The system is designed to build consumer, business and regulator trust in the cross-border flow of electronic personal data in the Asia-Pacific region. One of the goals of the CBPR system is to 'lift the overall standard of privacy protection throughout the [Asia-Pacific] region' through voluntary, enforceable standards set out within it.[13]

Organisations that choose to participate in the CBPR system must submit their privacy practices and policies for evaluation by an APEC-recognised Accountability Agent to assess compliance with the programme. Upon certification, the practices and policies will become binding on that organisation and enforceable through the relevant privacy enforcement authority.[14]

The CBPR system is governed by the Data Privacy Subgroup, which administers the programme through the Joint Oversight Panel, which is comprised of nominated representatives of participating economies and any working groups the Panel establishes. The Joint Oversight Panel operates according to the Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel and the Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel.[15]

Accountability Agents and privacy enforcement authorities are responsible for enforcing the CBPR programme requirements, either under contract (private Accountability Agents) or under applicable domestic laws and regulations (Accountability Agents and privacy enforcement authorities).

---

13 See: www.cbprs.org/Government/GovernmentDetails.aspx.

14 A privacy enforcement authority is 'any public body that is responsible for enforcing privacy law, and that has powers to conduct investigations or pursue enforcement proceedings'. 'Privacy law' is further defined as 'laws and regulations of an APEC economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework'. APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, at 10.

15 See: https://cbprs.blob.core.windows.net/files/JOP%20Charter.pdf; and also: https://cbprs.blob.core.windows.net/files/JOP%20Protocols.pdf.

The CBPR system has its own website that includes general information about the system, charters and protocols, lists of current participants and certified entities, submissions and findings reports, and template forms.[16]

Participation in the CBPR system

Only APEC member economies may participate in the CBPR system and must meet three requirements:

a participation in the APEC CPEA with at least one privacy enforcement authority;

b submission of a letter of intent to participate addressed to the chairs of the APEC ECSG, the Data Privacy Subgroup, and the CBPR system Joint Oversight Panel providing: (1) confirmation of CPEA participation; (2) identification of the APEC CBPR system recognised Accountability Agent that the economy intends to use; and (3) details regarding relevant domestic laws and regulations, enforcement entities, and enforcement procedures; and

c submission of the APEC CBPR system programme requirements enforcement map.

The Joint Oversight Panel of the CBPR issues a Findings Report that addresses whether the economy has met the requirements for becoming an APEC CBPR system participant. An applicant economy becomes a participant upon the date of a positive Findings Report.

Accountability Agents

The APEC CBPR system uses APEC-recognised Accountability Agents to review and certify participating organisations' privacy policies and practices as compliant with the APEC CBPR system requirements, including the APEC Privacy Framework. Applicant organisations may participate in the CBPR system only upon such certification, and it is the responsibility of the relevant Accountability Agent to undertake certification of an applicant organisation's compliance with the programme requirements. An Accountability Agent makes no determination as part of the CBPR verification programme regarding whether the applicant organisation complies with domestic legal obligations that may differ from the CBPR system requirements.

APEC CBPR system requirements for Accountability Agents include:

a being subject to the jurisdiction of a privacy enforcement authority in an APEC economy participating in the CBPR system;

b satisfying the Accountability Agent recognition criteria;[17]

c agreeing to use the CBPR intake questionnaire to evaluate applicant organisations (or otherwise demonstrate that propriety procedures meet the baseline requirements of the CBPR system); and

d completing and signing the signature and contact information form.[18]

16 See: www.cbprs.org/default.aspx.

17 See: https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Recognition%20Criteria.pdf.

18 See: https://cbprs.blob.core.windows.net/files/Signature%20and%20Contact%20Information.pdf.

Proposed Accountability Agents are nominated by an APEC member economy and, following an application and review process by the Joint Oversight Panel, may be approved by the ECSG upon recommendation by the Panel. Any APEC member economy may review the recommendation as to any proposed Accountability Agent and present objections to the ECSG. Once an application has been approved by the ECSG, then the Accountability Agent is deemed 'recognised'. Complaints about a recognised Accountability Agent are reviewed by the Joint Oversight Panel, which has the discretion to request investigative or enforcement assistance from the relevant privacy enforcement authority in the APEC economy where the agent is located.

No Accountability Agent may have an actual or potential conflict of interest nor may it provide services to entities it has certified or that have applied for certification. It must continue to monitor certified organisations for compliance with the APEC CBPR system standards and must obtain annual attestations regarding such compliance. It must publish its certification standards and must promptly report all newly certified entities, as well as any suspended or terminated entities to the relevant privacy enforcement authorities and the CBPR Secretariat.

Accountability Agents can be either public or private entities, and may also be a privacy enforcement authority. Under certain circumstances, an APEC economy may designate an Accountability Agent from another economy.

Accountability Agents are responsible for ensuring that any non-compliance is remedied in a timely fashion and reported, if necessary, to relevant enforcement authorities.

If only one Accountability Agent operates in an APEC economy and it ceases to function as an Accountability Agent for any reason, then the economy's participation in the CBPR system will be suspended and all certifications issued by that Accountability Agent for businesses will be terminated until the economy once again fulfils the requirements for participation and the organisations complete another certification process.

The CBPR system website contains a chart of recognised Accountability Agents, their contact information, date of recognition, approved APEC economies for certification purposes, and links to relevant documents and programme requirements.[19]

As of August 2015, the CBPR system recognised only one Accountability Agent: TRUSTe, recognised to certify only organisations subject to the jurisdiction of the United States Federal Trade Commission.

CBPR system compliance certification for organisations

Only organisations that are subject to the laws of one or more APEC CBPR system participating economies are eligible for certification regarding personal information transfers between economies.

An organisation that chooses to participate in the CBPR system initiates the process through submission of a self-assessment questionnaire and relevant documentation to an APEC-recognised Accountability Agent. The Accountability Agent will then undertake an iterative evaluation process to determine whether the organisation meets the baseline

19 See: www.cbprs.org/Agents/AgentDetails.aspx.

standards of the programme. The Accountability Agent has sole responsibility for these first two phases of the CBPR system accreditation process (self-assessment and compliance review).

Organisations that are found to be in compliance with the programme requirements will be certified as CBPR-compliant and identified on the CBPR website. As of August 2015, more than 20 organisations have been APEC CBPR certified, all of which are in the United States, with more in various stages of review.[20] Certified companies must undergo annual recertification. As more Accountability Agents are recognised in the economies participating in the CBPR system, the number of certified organisations is expected to grow.

Effect of the CBPR on domestic laws and regulations

The CBPR system sets a minimum standard for privacy protection requirements, and thus an APEC economy may need to make changes to its domestic laws, regulations and procedures to participate in the programme. With that exception, however, the CBPR system does not otherwise replace or modify any APEC economy's domestic laws and regulations. Indeed, if the APEC economy's domestic legal obligations exceed those of the CBPR system, then those laws will continue to apply to their full extent.

Privacy Recognition for Processors system

Because the CBPR system (and the APEC Framework) applies only to data controllers, who remain responsible for the activities done by processors on their behalf, APEC member economies and data controllers encouraged the development of a mechanism to help identify qualified and accountable data processors. This led, in 2015, to the APEC PRP programme, which is a mechanism by which data processors can be certified by an Accountability Agent.[21] Such certification can provide assurances to APEC economies and data controllers regarding the quality and compatibility of the processor's privacy policies and practices. The PRP does not change the allocation of responsibility for the processor's practices to the data controller, and there is no requirement that a controller engage a PRP-recognised processor to comply with the Framework's accountability principle.

APEC is in the process of integrating the PRP system into the CBPR governance system, and it is expected that the PRP system will follow the same model. Differences in national laws among APEC economies, however, necessarily result in different enforceability options under the PRP system, and how each economy will support enforcement is not yet finalised.

---

20 A current list of APEC-certified organisations can be found at: https://cbprs.blob.core.windows.net/files/APEC%20CBPR%20Compliance%20Directory_April2015.pdf.

21 The PRP Purpose and Background Document can be found at: https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf; and the intake questionnaire for processors is at: https://cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf.

iii The CPEA

One of the key goals of the Privacy Framework is to facilitate domestic and international efforts to promote and enforce information privacy protections. The Privacy Framework does not establish any central enforcement body but instead encourages the cooperation of privacy enforcement authorities within the Asia-Pacific region. APEC established the CPEA as a multilateral arrangement to facilitate such interaction. The CPEA became the first mechanism in the Asia-Pacific region to promote cooperative assistance among privacy enforcement authorities.

Among other things, the CPEA promotes voluntary information sharing and enforcement by:

a facilitating information sharing among privacy enforcement authorities within APEC member economies;

b supporting effective cross-border cooperation between privacy enforcement authorities through enforcement matter referrals, and parallel or joint enforcement actions; and

c encouraging cooperation and information sharing with enforcement authorities of non-APEC member economies.

The CPEA was endorsed by the APEC ministers in 2009 and commenced in 2010 with five participating economies: Australia, China, Hong Kong China, New Zealand and the United States. Any privacy enforcement authority from any APEC member economy may participate, and each economy may have more than one participating privacy enforcement authority. As of August 2015, CPEA participants included over two dozen Privacy Enforcement Authorities from nine APEC economies.[22]

Under the CPEA, any privacy enforcement authority may seek assistance from a privacy enforcement authority in another APEC economy by making a request for assistance. The receiving privacy enforcement authority has the discretion to decide whether to provide such assistance.

Participation in the CPEA is a prerequisite to participation by an APEC economy in the CBPR system. As a result, each participating APEC economy must identify an appropriate regulatory authority to serve as the privacy enforcement authority in the CBPR system. That privacy enforcement authority must be ready to review and investigate a CBPR complaint if it cannot be resolved by the certified organisation or the relevant Accountability Agent, and take whatever enforcement action is necessary and appropriate. As more member economies join the CBPR system, this enforcement responsibility is likely to become more prominent.

22 See: www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx for the most recent information about the CPEA and its participating privacy enforcement authorities.

IV INTEROPERABILITY

Given the global nature of personal information flows, APEC's Data Privacy Subgroup has been involved in collaborative efforts with other international organisations with the goal of improving trust and confidence in the protection of personal information and, ultimately, to enable the associated benefits of electronic commerce to flourish across the APEC region. While privacy regimes such as the APEC Privacy Framework are drafted at the level of principles, there are often very significant differences in the legal and policy implementation of those principles in different economies around the world. In an effort to bridge those differences and find commonality between the two largest privacy systems – the APEC Privacy Framework and the EU Data Protection Directive – in 2012 APEC endorsed participation in a working group to study the interoperability of the APEC and EU data privacy regimes.

In early 2014, the APEC/EU Working Group released a reference document (endorsed by APEC Senior Leaders in February 2014) that maps the CBPR system requirements and the binding corporate rules under the EU Data Protection Directive, and identifies commonalities and differences between the two (the Referential).[23] This document provides an important tool to multinational companies in developing global privacy compliance procedures that are compliant with both systems. Because it is set up in a block format, laying out the areas of commonality and the additional requirements of each privacy regime, the Referential provides a comparative tool that can be used as a checklist by companies seeking or considering certification by one or both systems. It does not, however, create interoperability or mutual recognition of the regimes.

The Referential points out that such companies still need to be approved by each of the respective bodies in both EU Member States and APEC economies. The Referential further cautions against using the document itself as an organisation's proposed framework because each organisation's privacy policies should be tailored to that organisation. Moreover, data processed in an APEC economy is still subject to that economy's domestic laws. And whenever the APEC CBPR system is incompatible with the EU Data Protection Directive, the organisation must affirmatively describe the circumstances under which it will apply the rules of one system rather than the other.

Following the Referential, the Article 29 Working Party and the APEC Data Privacy Subgroup agreed to develop additional practical tools to help organisations to become certified under both the BCR and CBPR systems. The joint working group has committed to developing a common application form based on each system's intake questionnaires that can be submitted, along with a mapping of the company policies and associated personal data and privacy programme practices and effectiveness tools, to support certification in both systems. The joint working group will also work, over the long term, to develop a common Referential for mapping requirements for processors under the BCR and CBPR systems.

23 See: www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

The Referential and the common application are important steps towards developing policies, practices and enforcement procedures that could apply to both systems, and perhaps – eventually – a common framework.

V THE YEAR IN REVIEW AND OUTLOOK

The Data Privacy Subgroup is undertaking a 10-year review and evaluation (stocktake) of domestic and international implementation of the APEC Privacy Framework through a working group established for that purpose and led by Australia. The member economies have been encouraged to update their IAPs in support of that stocktake. The stocktake will consider whether the APEC Privacy Framework should be updated to ensure relevance as the market evolves with technology innovations, such as big data, cloud computing and the internet of things. It will consider updating the Framework by addressing such topics as interoperability with other privacy frameworks, breach notification, privacy management programmes and factors to consider when balancing economic and privacy interests.

In February 2015, APEC announced the PRP system (see Section III.ii, *supra*), which is a set of baseline requirements that a data processor must meet to be certified by an Accountability Agent. With PRP, APEC's privacy certification programmes extends to cover the full scope of personal information collection and processing by both information controllers and processors. Data controllers can use certified processors to provide assurance of their ability to ensure that their privacy obligations are maintained through the entire personal information life cycle. Similarly, less-known processors within APEC economies may increase their global footprint by becoming certified.

On April 15, 2015, Canada joined the United States (2012), Mexico (2013) and Japan (2014) as an approved APEC economy participating in the APEC CBPR system. This system is growing slowly, as some economies are waiting to see interest from business, and some businesses are waiting for member economies to join. With all of the North American Free Trade Agreement countries participating, the CBPR system has made an important step towards an international presence, which may encourage more APEC member economies and business organisations to participate.

IBM became the first company to be certified under the APEC CBPR system, in August 2013; it has been joined by nearly two dozen others, including companies with significant international presence, such as Apple, HP, and Merck. All of these companies were certified by TRUSTe, the sole Accountability Agent to date.

TRUSTe became the first recognised Accountability Agent under the CBPR system on 25 June 2013, and that status was renewed unanimously by the 21 APEC member economies in early 2015. Mexico, Japan and Canada have not yet identified their domestic Accountability Agents.

Interoperability continues to be of significant interest. Following the publication of the Referential and in recognition of differences between the APEC CBPR system and the EU binding corporate rules, additional documentation and checklists will be developed to provide a resource to companies seeking approval and certification under both systems. This year, the BCR-CBPR joint working group examined case studies of companies that already have, or are in the process of seeking, certification under

both systems, to identify opportunities to streamline the process of dual certification or approval under both the BCR and CBPR systems. In a letter of 29 May 2015 to the APEC Data Privacy Subgroup Chair, the Article 29 Working Party Chair identified the agreed short-term action items for the joint working group as (1) developing a common BCR-CBPR application form that can be submitted to both European data protection authorities and APEC Accountability Agents and (2) developing compliance mapping tools with respect to both systems to be submitted in the joint application. The letter also agreed that the longer term goal of the joint working group was to develop a mapping document comparing the BCRs for processors and the APEC PRP.

Chapter 11

HONG KONG

Yuet Ming Tham and Jillian Lee[1]

I OVERVIEW

The Hong Kong legal framework concerning privacy, data protection and cybersecurity is consolidated under one piece of legislation, the Personal Data (Privacy) Ordinance (PDPO). All organisations that collect, hold, process or use personal data (data users) must comply with the PDPO and in particular, the six data protection principles (DPPs) in Schedule 1 of the PDPO, which are the foundation upon which the PDPO is based. The Office of the Privacy Commissioner for Personal Data (PCPD), an independent statutory body, was established to oversee the enforcement of the PDPO.

This chapter will discuss the recent data privacy developments, including new legislation and guidelines, and major enforcement actions in Hong Kong in 2015. It will also discuss the current data privacy regulatory framework in Hong Kong, and in particular, the six DPPs and their implications for organisations, as well as specific data privacy issues such as direct marketing, issues relating to technological innovation, international data transfer, cybersecurity and data breaches.

II THE YEAR IN REVIEW

i Proposed legislation and administrative measures

In December 2014, the PCPD published guidance on the protection of personal data in cross-border data transfers (the Guidance Note) to elaborate on the legal restrictions governing cross-border data transfers in Hong Kong, though the provision pertaining to the cross-border transfer of data has not actually entered into effect yet. Although the Hong Kong Personal Data (Privacy) Ordinance (the Ordinance) contains a provision (Section 33) imposing restrictions on cross-border data transfers, this provision did not

1 Yuet Ming Tham is a partner and Jillian Lee is an associate at Sidley Austin LLP.

enter into effect when the rest of the Ordinance was enacted in 1995. Consequently, there is currently no legal restriction on cross-border data transfers in Hong Kong; the new Guidance Note published by the Privacy Commissioner is voluntary and not binding.[2]

On 6 February 2015, the Legislative Council of Hong Kong introduced the Interception of Communications and Surveillance (Amendments) Bill 2015 (the Bill), which seeks to introduce amendments to the Interception of Communications and Surveillance Ordinance (Cap. 589) (ICSO). The Bill was introduced primarily to enlarge the supervisory powers of the Commissioner on Interception of Communications and Surveillance (CIS), and includes giving express power to the CIS to inspect protected products (i.e., interception and surveillance products).

On 31 March 2015, the PCPD published a Guidance on CCTV Surveillance and Use of Drones (the CCTV Guidance). This Guidance replaces the Guidance on CCTV Surveillance Practices as it introduces amendments to take account of the new provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012. More significantly, it incorporates new guidance for the responsible use of drones. The previous[3] Privacy Commissioner for Personal Data, Mr Allan Chiang, said, 'While the privacy implications of surveillance tools such as CCTV are fairly well understood, drones when fitted with cameras could add a new dimension to these privacy concerns by virtue of their unique attributes.' The privacy guidelines for the use of CCTV apply equally to the use of drones. Specific illustrations in the CCTV Guidance address drones' special attributes, such as mobility and small size.[4]

On 20 July 2015, the PCPD also published a Guidance on Collection and Use of Biometric Data to provide data users who intend to collect biometric data with practical guidance on complying with the requirements under the PDPO. This Guidance is prepared based on the knowledge and experience gained from relevant complaints or enquiries that the PCPD has handled. It replaces the previous Guidance Note on the Collection of Fingerprint Data, issued in May 2012.[5]

ii Data privacy complaints

A total of 1,690 complaints were received by the PCPD in 2014–2015, a 10 per cent decrease from the previous year. Although there has been an increase in the number of complaints in relation to the use of information and communications technology (ICT), the number of direct marketing-related complaints dropped as the public and organisations have become more familiar with the requirements under the new direct marketing regime.

---

2 www.pcpd.org.hk/english/resources_centre/publications/guidance/files/GN_crossborder_e.pdf.

3 On 4 August 2015, Mr Stephen Kai-yi Wong took office as the new Privacy Commissioner for Personal Data for a term of five years. (www.pcpd.org.hk/english/news_events/media_statements/press_20150804.html).

4 www.pcpd.org.hk/english/news_events/media_statements/press_20150331.html.

5 www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf.

The record-high 223 ICT-related complaints in 2014–2015 represented an 89 per cent year-on-year increase. Of these, 98 related specifically to use of social networks, 79 were about use of smartphone applications, 66 concerned disclosure or leakage of personal data on the internet, 34 involved cyberbullying and 11 related to other subtopics. The Privacy Commissioner sees the rising trend as principally attributable to the increasing popularity of smartphones and the internet.[6]

iii Enforcement actions

On 21 July 2015, it was reported by the PCPD that 42 employers were sanctioned for placing 46 job advertisements to solicit job applicants' personal data. These blind recruitment advertisements (blind ads) breached the fairness principle for personal data collection (DPP1(2) of the PDPO).[7] This year, the PCPD's investigations revealed that the blind ads situation has improved from 2014, when it conducted a compliance survey of recruitment advertisements on seven major recruitment media. From 3 to 9 May 2015, 12,849 advertisements placed in the same seven recruitment media were examined and only 59 blind ads were identified. Overall, the proportion of blind ads has dropped from 3.45 per cent (2014) to 0.46 per cent (2015).

On 21 July 2015, the PCPD also published an investigation report on Queenix (Asia) Limited, a fashion trading company. The PCPD considered the company's collection of employees' fingerprint data (for the purpose of safeguarding office security and monitoring staff attendance) excessive and unfair.[8] An enforcement notice was served on the company directing it to destroy all fingerprint data collected.

iv Increasing public awareness

In January 2015, the PCPD launched a privacy awareness campaign with the theme 'Developing Mobile Apps: Privacy Matters'. The former Privacy Commissioner for Personal Data, Mr Allan Chiang, mentioned during the campaign inauguration ceremony that it is the PCPD's aim to embrace the next wave of ICT advancements, so as to enhance economic and social development. However, Mr Chiang also emphasised that consumer privacy and data security remain PCPD's priority.[9]

On 31 July 2015, the PCPD also released a revised information leaflet entitled 'Protect Privacy by Smart Use of Smartphones' to help smartphone users minimise the personal data privacy risks associated with the use of smartphones.[10]

---

6 www.pcpd.org.hk/english/resources_centre/publications/annual_report/files/anreport15_03.pdf.

7 www.pcpd.org.hk/english/news_events/media_statements/press_20150721a.html.

8 www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R15_2308_e.pdf.

9 www.pcpd.org.hk/english/news_events/media_statements/press_20150108.html.

10 www.pcpd.org.hk/english/news_events/media_statements/press_20150731.html.

III REGULATORY FRAMEWORK

i The PDPO and the six DPPs

The PDPO entered into force on 20 December 1996 and it was recently amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance). The majority of the provisions of the Amendment Ordinance entered into force on 1 October 2012 and the provisions relating to direct marketing and legal assistance entered into force on 1 April 2013.

The PCPD has issued various codes of practice and guidelines to provide organisations with practical guidance to comply with the provisions of the PDPO. Although the codes of practice and guidelines are only issued as examples of best practice and organisations are not obliged to follow them, in deciding whether an organisation is in breach of the PDPO, the Privacy Commissioner will take into account various factors, including whether the organisation has complied with the codes of practice and guidelines published by the PCPD. In particular, failure to abide by certain mandatory provisions of the codes of practice will weigh unfavourably against the organisation concerned in any case that comes before the Privacy Commissioner. In addition, a court is entitled to take that fact into account when deciding whether there has been a contravention of the PDPO.

As mentioned above, the six DPPs of the PDPO set out the basic requirements with which data users must comply in the handling of personal data. Most of the enforcement notices served by the PCPD relate to contraventions of the six DPPs. Although a contravention of the DPPs does not constitute an offence, the PCPD may serve an enforcement notice on data users for contravention of the DPPs and a data user who contravenes an enforcement notice commits an offence.

DPP1 – Purpose and manner of collection of personal data

Principle

DPP1 provides that personal data shall only be collected if it is necessary for a lawful purpose directly related to the function or activity of the data user. Further, the data collected must be adequate but not excessive in relation to that purpose.

Data users are required to take all practicable steps to ensure that on or before the collection of the data subjects' personal data (or on or before first use of the data in respect of item (d) below), the data subjects were informed of the following matters:

a the purpose of collection;

b the classes of transferees of the data;

c whether it is obligatory to provide the data; and if so, the consequences of failing to supply the data; and

d the right to request access to and request the correction of the data, and the contact details of the individual who is to handle such requests.

Implications for organisations

A personal information collection statement (PICS) (or its equivalent) is a statement given by a data user for the purpose of complying with the above notification requirements. It is crucial that organisations provide a PICS to their customers before collecting their personal data. On 29 July 2013 the PCPD published the Guidance on Preparing

Personal Information Collection Statement and Privacy Policy Statement, which serves as a guidance for data users when preparing their PICS. It is recommended that the statement in the PICS explaining what the purpose of the collection is should not be too vague and too wide in scope, and the language and presentation of the PICS should be user-friendly. Further, if there is more than one form for collection of personal data each serving a different purpose, the PICS used for each form should be tailored to the particular purpose.

DPP2 – Accuracy and duration of retention

Principle

Under DPP2, data users must ensure that the personal data that they hold is accurate and up-to date and is not kept longer than necessary for the fulfilment of the purpose.

After the Amendment Ordinance came into force, it is provided under DPP2 that if a data user engages a data processor, whether within or outside Hong Kong, the data users must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than necessary for processing the data. 'Data processor' is defined to mean a person who processes personal data on behalf of a data user and does not process the data for its own purposes.

It should be noted that under Section 26 of the PDPO, a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased. Contravention of this Section is an offence and the offenders are liable for a fine.

Implications for organisations

The PCPD published the Guidance on Personal Data Erasure and Anonymisation (revised on April 2014), which provides advice on when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and physical destruction. For example, it is recommended that dedicated software such as those conforming to industry standards (e.g., US Department of Defense deletion standards) be used to permanently delete data on various types of storage devices. Organisations are also advised to adopt a top-down approach in respect of data destruction and this requires the development of organisation-wide policies, guidelines and procedures. Apart from data destruction, the guidance note also provides that the data can be anonymised to the extent that it is no longer practicable to identify an individual directly or indirectly. In such cases, the data would no longer be considered as 'personal data' under the PDPO. Nevertheless, it is recommended that data users must still conduct a regular review to confirm whether the anonymised data can be re-identified and to take appropriate actions to protect the personal data.

DPP3 – Use of personal data

Principle

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. 'Prescribed consent' means express consent given voluntarily and that has not been withdrawn by notice in writing.

Implications for organisations

Organisations should only use, process or transfer their customers' personal data in accordance with the purpose and scope set out in their PICS. If the proposed use is likely to fall outside the customers' reasonable expectation, organisations should obtain express consent from their customers before using their personal data for a new purpose.

DPP4 – Data security requirements

Principle

DPP4 provides that data users must use all practicable steps to ensure that personal data held are protected against unauthorised or accidental processing, erasure, loss or use.

After the Amendment Ordinance came into force, it is provided under DPP4 that if a data user engages a data processor (such as a third-party IT provider to process personal data of employees or customers), whether within or outside Hong Kong, the data users must adopt contractual or other protections to ensure the security of the data. This is important because under Section 65(2) of the PDPO, the data user is liable for any act done or practice engaged in by its data processor.

Implications for organisations

In view of the increased use of third-party data centres and the growth of IT outsourcing, the PCPD issued an information leaflet entitled 'Outsourcing the Processing of Personal Data to Data Processors', dated September 2012. According to the information leaflet, it is recommended that data users incorporate contractual clauses in their service contracts with data processors to impose obligations on them to protect the personal data transferred to them. Other protection measures include selecting reputable data processors and conducting audits or inspections of the data processors.

The PCPD also issued the Guidance on the Use of Portable Storage Devices (revised in July 2014), which helps organisations to manage the security risks associated with the use of portable storage devices. Portable storage devices include USB flash cards, tablets or notebook computers, mobile phones, smartphones, portable hard drives, DVDs, etc. Given that large amounts of personal data can be quickly and easily copied to such devices, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policies and practice. The guidance note recommended that a risk assessment be carried out to guide the development of an organisation-wide policy to manage the risk associated with the use of portable storage devices. Further, given the rapid development of technology, it is recommended that this policy be updated and audited regularly. Some technical controls recommended by the guidance note include encryption of the personal data stored on the personal storage devices and adopting systems that detect and block the saving of sensitive information to external storage devices.

DPP5 – Privacy policies

Principle

DPP5 provides that data users must publicly disclose the kind of personal data held by them, the main purposes for holding the data, and their policies and practices on how they handle the data.

Implications for organisations

A privacy policy statement (PPS) (or its equivalent) is a general statement about a data user's privacy policies for the purpose of complying with DPP5. Although the PDPO is silent on the format and presentation of a PPS, it is good practice for organisations to have a written policy to effectively communicate their data management policy and practice. The PCPD published a guidance note entitled Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PPS. In particular, it is recommended that the PPS should be in a user-friendly language and presentation. Further, if the PPS is complex and lengthy, the data user may consider using proper headings and adopting a layered approach in presentation.

DPP6 – Data access and correction

Principle

Under DPP6, a data subject is entitled to ascertain whether a data user holds any of his or her personal data, and to request a copy of the personal data. The data subject is also entitled to request the correction of his or her personal data if the data is inaccurate.

Data users are required to respond to a data access or correction request within a statutory period of 40 days. If the data user does not hold the requested data, it must still inform the requestor that it does not hold the data within 40 days.

Given that a substantial number of disputes under the PDPO relate to data access requests, the PCPD published a guidance note entitled Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users, dated June 2012, to address the relevant issues relating to requests for data access. For example, although a data user may impose a fee for complying with a data access request, a data user is only allowed to charge the requestor for the costs that are 'directly related to and necessary for' complying with a data access request. It is recommended that a data user should provide a written explanation of the calculation of the fee to the requestor if the fee is substantial. Further, a data user should not charge a data subject for its costs in seeking legal advice in relation to the compliance of the data access request.

ii Direct marketing

New direct marketing provisions under the PDPO

The new direct marketing provisions under the Amendment Ordinance entered into effect on 1 April 2013 and introduced a stricter regime that regulates the collection and use of personal data for sale and for direct marketing purposes.

Under the new direct marketing provisions, data users must obtain the data subjects' express consent before they use or transfer the data subjects' personal data for direct marketing purposes. Organisations must provide a response channel (e.g., email, online facility or a specific address to collect written response) to the data subject through which the data subjects may communicate their consent to the intended use. Transfer of personal data to another party (including the organisation's subsidiaries or affiliates) for direct marketing purposes, whether for gain or not, will require express written consent from the data subjects.

New Guidance on Direct Marketing

The PCPD published the New Guidance on Direct Marketing in January 2013 to assist businesses to comply with the requirements of the new direct marketing provisions of the PDPO.

Direct marketing to corporations

Under the New Guidance on Direct Marketing, the Privacy Commissioner stated that in clear-cut cases where the personal data is collected from individuals in their business or employee capacities and the product or service is clearly meant for the exclusive use of the corporation, the Commissioner will take the view that it would not be appropriate to enforce the direct marketing provisions.

The Privacy Commissioner will consider the following factors in determining whether the direct marketing provisions will be enforced:

a the circumstances under which the personal data is collected, for example, whether the personal data concerned is collected in the individual's business or personal capacity;

b the nature of the products or services, namely, whether they are for use of the corporation or for personal use; and

c whether the marketing effort is targeted at the business or the individual.

Amount of personal data collected

While the Privacy Commissioner has expressed that the name and contact information of a customer should be sufficient for the purpose of direct marketing, it is provided in the New Guidance on Direct Marketing that additional personal data may be collected for direct marketing purposes (e.g., customer profiling and segmentation) if the customer elects to supply the data on a voluntary basis. Accordingly, if an organisation intends to collect additional personal data from its customers for direct marketing purposes, it must inform its customers that the supply of any other personal data to allow it to carry out specific purposes, such as customer profiling and segmentation, is entirely voluntary, and obtain written consent from its customers for such use.

Penalties for non-compliance

Non-compliance with the direct marketing provisions of the PDPO is an offence and the highest penalties are a fine of HK$1 million and imprisonment for five years. At the time of writing, the PCPD has not published any cases relating to contravention of the new direct marketing provisions and it remains to be seen how the new direct marketing provisions will be enforced by the PCPD.

Spam messages

Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the Unsolicited Electronic Messages Ordinance (UEMO). Under the UEMO, businesses must not send commercial electronic messages to any telephone or fax number registered in the do-not-call registers. This includes text messages sent via SMS, pre-recorded phone messages, faxes and emails. Contravention of the UEMO may result in fines ranging from HK$100,000 to HK$1 million and up to five years' imprisonment.

In early 2014, the Office of the Communications Authority prosecuted a travel agency for sending commercial facsimile messages to telephone numbers registered in the do-not-call registers. This is the first prosecution since the UEMO came into force in 2007. The case was heard before a magistrate's court but the defendant was not convicted because of a lack of evidence.

Person-to-person telemarketing calls

Although the Privacy Commissioner has previously proposed to set up a territory-wide do-not-call register on person-to-person telemarketing calls, this has not been pursued by the government in the recent amendment of the PDPO.[11] Nevertheless, under the new direct marketing provisions of the PDPO, organisations must ensure that they do not use the personal data of customers or potential customers to make telemarketing calls without their consent. Organisations should also check that the names of the customers who have opted out from the telemarketing calls are not retained in their call lists.

On 5 August 2014, the Privacy Commissioner made a media brief to urge the government administration to amend the UEMO to expand the do-not-call registers to include person-to-person calls. In support of the amendment, the Privacy Commissioner conducted a public opinion survey, which revealed that there had been a growing incidence of person-to-person calls, with more people responding negatively to the calls and fewer people reporting any gains from the calls. Although there had been long-standing discussions regarding the regulation of person-to-person calls in the past, it remains to be seen whether any changes will be made to the legislation.

iii Technological innovation and privacy law

Cookies, online tracking and behavioural advertising

While there are no specific requirements in Hong Kong regarding the use of cookies, online tracking or behavioural advertising, organisations that deploy online tracking that involves the collection of personal data of website users must observe the requirements under the PDPO, including the six DPPs.

The PCPD published an information leaflet entitled 'Online Behavioural Tracking' (revised in April 2014), which provides the recommended practice for organisations that deploy online tracking on their websites. In particular, organisations are recommended to inform users what types of information are being tracked by them, whether any third party is tracking their behavioural information and to offer users a way to opt out of the tracking.

In cases where cookies are used to collect behavioural information, it is recommended that organisations preset a reasonable expiry date for the cookies, encrypt the contents of the cookies whenever appropriate and not deploy techniques that ignore browser settings on cookies unless they can offer an option to website users to disable or reject such cookies.

11 Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance (April 2011).

The PCPD also published the Guidance for Data Users on the Collection and Use of Personal Data through the Internet (revised in April 2014), which advises organisations on compliance with the PDPO while engaging in the collection, display or transmission of personal data through the internet.

Cloud computing

The PCPD published the information leaflet 'Cloud Computing' in November 2012, which provides advice to organisations on the factors they should consider before engaging in cloud computing. For example, organisations should consider whether the cloud provider has subcontracting arrangements with other contractors and what measures are in place to ensure compliance with the PDPO by these subcontractors and their employees. Also, when dealing with cloud providers that offer only standard services and contracts, the data user must evaluate whether the services and contracts meet all security and personal data privacy protection standards they require.

On 30 July 2015, the PCPD published the revised information leaflet, 'Cloud Computing', to advise cloud users on privacy, the importance of fully assessing the benefits and risks of cloud services and the implications for safeguarding personal data privacy. The new leaflet includes advice to organisations on what types of assurances or support they should obtain from cloud service providers to protect the personal data entrusted to them.

Employee monitoring

The PCPD published the Privacy Guidelines: Monitoring and Personal Data Privacy at Work to aid employers in understanding steps they can take to assess the appropriateness of employee monitoring. The guidelines are applicable to monitoring by telecommunications equipment (e.g., telephones, computers, mobile phones), company email services, internet browsing, video recording and closed-circuit TV systems.

Employers must ensure that they do not contravene the DPPs of the PDPO while monitoring employees' activities. In particular, employers must ensure that:

a monitoring is only carried out to the extent necessary to deal with their legitimate business purpose;

b the personal data collected in the course of monitoring is kept to an absolute minimum and by means that are fair in the circumstances; and

c a written privacy policy on employee monitoring has been implemented and practicable steps have been taken to communicate that policy to employees.

IV INTERNATIONAL DATA TRANSFER

Section 33 of the PDPO deals with the transfer of data outside Hong Kong and it prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances, such as where the data protection laws of the foreign country are similar to the PDPO or the data subject has consented to the transfer in writing.

Section 33 of the PDPO has not been brought into force since its enactment in 1995 and the government currently has no timetable for its implementation. However, given the increased level of activity by the PCPD, it is foreseeable that Section 33 will be implemented eventually.

V COMPANY POLICIES AND PRACTICES

Organisations that handle personal data are required to provide their PPS to the public in an easily accessible manner. In addition, prior to collecting personal data from individuals, organisations must provide a PICS setting out, among other things, the purpose of collecting the personal data and the classes of transferees of the data. As mentioned above, the PCPD has published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement (see Section III.i, *supra*), which provides guidance for organisations when preparing their PPS and PICS.

The Privacy Management Programme: A Best Practice Guide (see Section II.i, *supra*) also provides guidance for organisations to develop their own privacy policies and practices. In particular, it is recommended that organisations should appoint a data protection officer to oversee the organisation's compliance with the PDPO. In terms of company policies, apart from the PPS and PICS, the Best Practice Guide recommends that organisations develop key policies on the following areas:

a accuracy and retention of personal data;
b security of personal data; and
c access to and correction of personal data.

The Best Practice Guide also emphasises the importance of ongoing oversight and review of the organisation's privacy policies and practices to ensure they remain effective and up to date.

VI DISCOVERY AND DISCLOSURE

i Discovery

The use of personal data in connection with any legal proceedings in Hong Kong is exempted from the requirements of DPP3, which requires organisations to obtain prescribed consent (see Section III.i, *supra*) from individuals before using their personal data for a new purpose. Accordingly, the parties in legal proceedings are not required to obtain consent from the individuals concerned before disclosing documents containing their personal data for discovery purposes during legal proceedings.

ii Disclosure

Regulatory bodies in Hong Kong such as the Hong Kong Police Force, the Independent Commission Against Corruption and the Securities and Futures Commission are obliged to comply with the requirements of the PDPO during their investigations. For example, regulatory bodies in Hong Kong are required to provide a PICS to the individuals prior to collecting information or documents containing their personal data during investigations.

Nevertheless, in certain circumstances, organisations and regulatory bodies are not required to comply with DPP3 to obtain prescribed consent from the individuals concerned. This includes cases where the personal data is to be used for the prevention or detection of crime and the apprehension, prosecution or detention of offenders, and where the compliance with DPP3 would likely prejudice the aforesaid purposes.

Another exemption from DPP3 is where the personal data is required by or authorised under any enactment, rule of law or court order in Hong Kong. For example, the Securities and Futures Commission may issue a notice to an organisation under the Securities and Futures Ordinance requesting the organisation to produce certain documents that contain its customers' personal data. In such a case, the disclosure of the personal data by the organisation would be exempted from DPP3 because it is authorised under the Securities and Futures Ordinance.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Public enforcement

An individual may make a complaint to the PCPD about an act or practice of a data user relating to his or her personal data. If the PCPD has reasonable grounds to believe that a data user may have breached the PDPO, the PCPD must investigate the relevant data user. As mentioned above, although a contravention of the DPPs does not constitute an offence in itself, the PCPD may serve an enforcement notice on data users for contravention of the DPPs and a data user who contravenes an enforcement notice commits an offence.

Prior to the amendment of the PDPO in 2012, the PCPD was only empowered to issue an enforcement notice where, following an investigation, it is of the opinion that a data user is contravening or is likely to continue contravening the PDPO. Accordingly, in previous cases where the contraventions had ceased and the data users had given the PCPD written undertakings to remedy the contravention and to ensure that the contravention would not continue or recur, the PCPD could not serve an enforcement notice on them as continued or repeated contraventions were unlikely.

Since the entry into force of the Amendment Ordinance, the PCPD has been empowered to issue an enforcement notice where a data user is contravening, or has contravened the PDPO, regardless of whether the contravention has ceased or is likely to be repeated. According to the PCPD's 2013 review, the number of enforcement notices served by the PCPD has more than doubled compared with 2012, and this could be attributed to the enhanced power of the PCPD to take such enforcement actions under the Amendment Ordinance.

The enforcement notice served by the PCPD may direct the data user to remedy and prevent any recurrence of the contraventions. A data user who contravenes an enforcement notice commits an offence and is liable on first conviction for a fine of up to HK$50,000 and two years' imprisonment and, in the case of a continuing offence, a penalty of HK$1,000 for each day on which the offence continues. On second or subsequent conviction, the data user would be liable for a fine of up to HK$100,000 and imprisonment for two years, with a daily penalty of HK$2,000.

ii Private enforcement

Section 66 of the PDPO provides for civil compensation. Individuals who suffer loss as a result of a data user's use of their personal data in contravention of the PDPO are entitled to compensation by that data user. It is a defence for data users to show that they took reasonable steps to avoid such a breach.

After the Amendment Ordinance came into force, affected individuals seeking compensation under Section 66 of the PDPO may apply to the Privacy Commissioner for assistance and the Privacy Commissioner has discretion whether to approve it. Assistance by the Privacy Commissioner may include giving advice, arranging assistance by a qualified lawyer, arranging legal representation or other forms of assistance that the Privacy Commissioner may consider appropriate. According to the PCPD's 2013 review, the PCPD received 16 applications in 2013. Of these applications, one was granted assistance, five were rejected and two were withdrawn by the applicants.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Although the PDPO does not confer extraterritorial application, it applies to foreign organisations to the extent where the foreign organisations have offices or operation in Hong Kong. For example, if a foreign company has a subsidiary in Hong Kong, the Hong Kong subsidiary will be responsible for the personal data that it controls and it must ensure the personal data are handled in accordance with the PDPO, no matter whether the data is transferred back to the foreign parent company for processing.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

Legislative enactments relating to cybersecurity in Hong Kong are dealt with by both the PDPO and the criminal law.

The Computer Crimes Ordinance was enacted in 1993, and it has, through the amendment of the Telecommunications Ordinance,[12] the Crimes Ordinance[13] and the Theft Ordinance,[14] expanded the scope of existing criminal offences to include computer-related criminal offences. These include unauthorised access to any computer; damage or misuse of property (computer program or data); making false entries in banks' books of accounts by electronic means; obtaining access to a computer with intent to commit an offence or with dishonest intent; and unlawfully altering, adding or erasing the function or records of a computer.

12 Sections 24 and 27 of the Telecommunications Ordinance.

13 Sections 59, 60, 85 and 161 of the Crimes Ordinance.

14 Sections 11 and 19 of the Theft Ordinance.

ii Data breaches

There is currently no mandatory data breach notification requirement in Hong Kong. The PCPD published Guidance on Data Breach Handling and the Giving of Breach Notifications in June 2010, which provides data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the individuals involved. In particular, after assessing the situation and the impact of the data breach, the data users should consider whether the following persons should be notified as soon as practicable:

a the affected data subjects;
b the law enforcement agencies;
c the Privacy Commissioner (a data breach notification form is available from the PCPD's website);
d any relevant regulators; or
e other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the data subjects affected (for example, internet companies such as Google and Yahoo may assist in removing the relevant cached link from their search engines).

X OUTLOOK

Recent trends clearly indicate the development of a stricter privacy regulatory regime in Hong Kong, with closer scrutiny and an increase in the number of enforcement actions by the Privacy Commissioner. As previously mentioned, although Section 33 has yet to enter into force, the introduction of the Guidance Note may itself signal that Section 33 could soon be implemented. Due to the significant penalties for breach of Section 33, IT organisations doing business in Hong Kong should ensure that they commence a review of their business and international data transfer processes to meet the standards set out in the PDPO and DPPs. A robust data privacy compliance programme will also be required to meet the growing requirements of company data privacy policies and to keep pace with legislative and technological developments.

Chapter 16

JAPAN

Takahiro Nonaka[1]

I OVERVIEW

In Japan, the Act on the Protection of Personal Information[2] (APPI) primarily handles the protection of data privacy issues. The APPI applies to business operators that have used any personal information database containing details of more than 5,000 persons on any day in the past six months.[3]

Approximately 40 guidelines regarding personal information protection have been issued by government agencies including the Ministry of Health, Labour and Welfare,[4] the Japan Financial Services Agency[5] and the Ministry of Economy, Trade and Industry.[6] These guidelines prescribe in detail the interpretations and practices of the APPI in relevant industries.

---

1 Takahiro Nonaka is a counsel at Sidley Austin Nishikawa Foreign Law Joint Enterprise.

2 Act No. 57 of 30 May 2003, enacted on 30 May 2003 except for Chapters 4 to 6 and Articles 2 to 6 of the Supplementary Provisions, completely enacted on 1 April 2005 and amended by Act No. 49 of 2009: www.caa.go.jp/planning/kojin/foreign/act_1.pdf.

3 Article 2 of the Order for Enforcement of the Act on the Protection of Personal Information (Cabinet Order 506, 2003, enacted on 10 December 2003). Under the revised APPI, this minimum requirement is deleted.

4 The Guidelines on Protection of Personal Information in the Employment Management (Announcement No. 357 of 14 May 2012 by the Ministry of Health, Labour and Welfare).

5 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement No. 63 of 20 November 2009 by the Financial Services Agency).

6 The Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information (Announcement No. 2 of 9 October 2009 by

II THE YEAR IN REVIEW

i Policy Outline of the Institutional Revision for Use of Personal Data, and the revision of the APPI

On 24 June 2014, the Japanese government[7] published the Policy Outline of the Institutional Revision for Use of Personal Data.[8] The Policy Outline shows the government's direction on which measures are to be taken to amend the APPI and the other personal information protection-related laws. The revision bill of the APPI passed the Diet on 3 September 2015. The main changes proposed in the Policy Outline, which underlies the revision of the APPI, are set out below. A brief summary of the revision is given in Section X, *infra*.

Development of a third-party authority system[9]

The government will develop an independent government body to serve as a data protection authority to operate ordinances and self-regulation in the private sector to promote the use of personal data. The primary amendments to the system are as follows:

a the government will develop the structure of the third-party authority ensuring international consistency, so that legal requirements and self-regulation in the private sector are effectively enforced;

b the government will restructure the Specific Personal Information Protection Commission prescribed in the Number Use Act[10] to set up a commission for the purpose of promoting a balance between the protection of personal data and effective use of personal data; and

c the third-party authority shall have the functions and powers of on-site inspection, in addition to the functions and powers that the competent ministers currently have over businesses handling personal information, and shall certify non-governmental self-regulation and certify or supervise non-governmental organisations that conduct conformity assessment in accordance with the privacy protection standards adopted by the country concerned regarding international transfer of personal data.

---

the Ministry of Health, Labour and Welfare and the Ministry of Economy, Trade and Industry) (the Economic and Industrial Guidelines): www.meti.go.jp/policy/it_policy/privacy/0708english.pdf.

7 Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society.

8 http://japan.kantei.go.jp/policy/it/20140715_2.pdf.

9 The European Commission pointed out the lack of a data protection authority in the Japanese system in its 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, B-5: Japan', Graham Greenleaf, 20 January 2010 (the EC Comparative Study).

10 Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013). See Section II.ii, *infra*.

Actions for globalisation

If businesses handling personal data are planning to provide personal data (including personal data provided by overseas businesses and others) to overseas businesses, they have to take action, such as concluding a contract, so that overseas businesses to which personal data will be provided take the necessary and appropriate actions that are compatible with technological development for the safe management of personal data. In addition, the government will consider the details of actions based on the types of data transfer and a framework for ensuring their effectiveness. Also, the government will establish a framework for non-governmental organisations that are certified by the third-party authority to certify businesses that are planning to distribute data across borders, examining their compliance with the privacy protection standards acknowledged by the countries concerned.

Framework for promoting the use of personal data (big data issues)

The use of personal data is expected to create innovation with the multidisciplinary utilisation of diverse and vast amounts of data thereby creating new businesses. The current system of the APPI requires consent from persons to use their personal data for purposes other than those specified. Providing personal data to third parties is cumbersome for businesses, and creates a barrier to the use of personal data. Because the consent of the person is required to prevent a violation of personal rights and interests, the government will in the future implement a new framework to enable personal data to be provided to third parties without their consent to promote the use of personal data but prohibiting the identification of specific individuals.

Sensitive personal information

The APPI does not currently define 'sensitive personal information'; however, according to the Policy Outline, the amendments to the APPI will define information regarding an individual's race, creed, social status, criminal record and past record as sensitive personal information, along with any other information that may cause social discrimination.

The government will consider measures on the handling of sensitive information, such as prohibiting such data from being handled if it is included in personal information.

The Policy Outline also mentions that in view of the actual use of personal information including sensitive information and the purpose of the current law, the government will lay down regulations regarding the handling of personal information, such as providing exceptions where required according to laws and ordinances and for the protection of human life, health or assets, as well as enabling personal information to be obtained and handled with consent of the persons concerned.

In this regard, there is currently no provision that specifically addresses consent requirements for sensitive personal information in the APPI; instead these are regulated by a number of guidelines issued by government ministries (see, for example, Section III.i.(e), *infra*).

ii Social security numbers

The bill on the use of numbers to identify specific individuals in administrative procedures (the Number Use Act, also called the Social Security and Tax Number Act) was enacted

on 13 May 2013[11] and provides for the implementation of a national numbering system of social security and taxation purposes. The Japanese government will adopt the social security and tax number system to: (1) enhance social security for people who truly need it; (2) achieve the fair distribution of burdens such as income tax payments; and (3) develop efficient administration. An independent supervisory authority called the Specific Personal Information Protection Commission will be established. This authority will consist of one chairman and six commission members. The chairman and commissioners will be appointed by Japan's Prime Minister, and confirmed by the National Diet. The numbering system will be in effect from January 2016. Unlike other national ID numbering systems, Japan has not set up a centralised database for the numbers because of concerns about data breaches and privacy.

iii Online direct marketing

Under the Act on Regulation of Transmission of Specified Electronic Mail[12] and the Act on Specified Commercial Transactions,[13] businesses are generally required to provide recipients with an opt-in mechanism, namely to obtain prior consent from each recipient for any marketing messages sent by electronic means. A violation of the opt-in obligation may result in imprisonment, a fine or both.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Definitions

a Personal information:[14] information about a living person that can identify him or her by name, date of birth or other description contained in such information (including information that will allow easy reference to other information that will enable the identification of the specific individual).

b Personal information database:[15] an assembly of information including:

- information systematically arranged in such a way that specific personal information can be retrieved by a computer; or
- in addition, an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved.

11 The revision bill of the Number Use Act passed on 3 September 2015. The purpose of this revision is to provide further uses of the numbering system (i.e., management of personal medical history).

12 Act No. 26 of 17 April 2002.

13 Act No. 57 of 4 June 1976.

14 Article 2(1) APPI.

15 Article 2(2) APPI.

c A business operator handling personal information:[16] a business operator using a personal information database, etc., for its business.[17] However, the following entities shall be excluded:
- state organs;
- local governments;
- incorporated administrative agencies, etc.;[18]
- local incorporated administrative institutions;[19] and
- entities specified by a Cabinet Order as having little likelihood of harming the rights and interests of individuals considering the volume and the manner of use of personal information they handle.[20]

d Personal data:[21] personal information constituting a personal information database, etc. (when personal information such as name and addresses is compiled as a database it is 'personal data' in terms of the APPI).

e Sensitive personal information: the APPI itself does not have a definition of sensitive personal information (see Section II.i, *supra*). However, for example, the Japan Financial Services Agency's Guidelines for Personal Information Protection in the Financial Field (JFSA Guidelines)[22] define information related to political opinion, religious belief (religion, philosophy, creed), participation in a trade union, race, nationality, family origin, legal domicile, medical care, sexual life and criminal record as sensitive information.[23] The JFSA Guidelines prohibit the collection, use or provision to a third party of sensitive information,[24] although some exceptions exist.

16 Article 2(3) APPI.

17 The APPI applies to business operators that use any personal information database containing details of more than 5,000 persons on any day in the past six months. See footnote 3, *supra*.

18 Which means independent administrative agencies as provided in Paragraph (1) of Article 2 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 59 of 2003).

19 Which means local incorporated administrative agencies as provided in Paragraph (1) of Article 2 of the Local Incorporated Administrative Agencies Law (Act No. 118 of 2003).

20 Under the revised APPI, this exception is deleted. See footnote 3, *supra*.

21 Article 2(4) APPI.

22 The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information (Announcement No. 63 of 20 November 2009 by the Financial Services Agency).

23 Article 6(1) of the JFSA Guidelines.

24 Article 6(1)1–8 of the JFSA Guidelines.

ii General obligations for data handlers

Purpose of use

Pursuant to Article 15(1) APPI, a business operator handling personal information must as far as possible specify the purpose of that use. In this regard, the Basic Policy on the Protection of Personal Information (the Basic Policy) (Cabinet Decision of 2 April 2004) prescribes as follows:

> *To maintain society's trust of business activities, it is important for businesses to announce their appropriate initiatives for complaint processing and not using personal information for multiple uses through the formulation and announcement of their policies (so-called privacy policies or privacy statements, etc.) and philosophies on the promotion of the personal information protection. It is also important for businesses to externally explain, in advance and in an easy-to-understand manner, their procedures relating to the handling of personal information, such as notification and announcement of the purpose of use and disclosure, etc., as well as comply with the relevant laws and ordinances.*

To this end the Economic and Industrial Guidelines specifically prescribe the recommended items that should be included in privacy policies or privacy statements.

The government has formulated the Basic Policy, based on Article 7, Paragraph 1 APPI. To provide for the complete protection of personal information, the Basic Policy shows the orientation of measures to be taken by local public bodies and other organisations, such as businesses that handle personal information, as well as the basic direction concerning the promotion of measures for the protection of personal information and the establishment of measures to be taken by the state. This government Basic Policy requires a wide range of government and private entities to take specific measures for the protection of personal information.

Also, a business operator handling personal information must not change the use of personal information beyond a reasonable extent. The purpose of use after the change must therefore be duly related to that before the change.[25]

In addition, a business operator handling personal information must not handle personal information about a person beyond the scope necessary for the achievement of the purpose of use, without obtaining the prior consent of the person.[26]

Proper acquisition of personal information and notification of purpose

A business operator handling personal information shall not acquire personal information by a deception or other wrongful means.[27]

25 Article 15(2) APPI.

26 Article 16(1) APPI.

27 Article 17 APPI.

Also, having acquired personal information, a business operator handling personal information must promptly notify the data subject of the purpose of use of that information or publicly announce the purpose of use, except in cases in which the purpose of use has already been publicly announced.[28]

Maintenance of the accuracy of data and supervision of employees or outsourcing contractors

A business operator handling personal information must endeavour to keep any personal data it holds accurate and up to date within the scope necessary for the achievement of the purpose of use.[29]

In addition, when a business operator handling personal information has an employee handle personal data, it must exercise necessary and appropriate supervision over the employee to ensure the secure control of the personal data.[30]

Also, when a business operator handling personal information entrusts another individual or business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the outsourcing contractor to ensure the security control of the entrusted personal data.[31]

Restrictions on provision to a third party

In general, a business operator handling personal information must not provide personal data to a third party without obtaining the prior consent of the data subject.[32]

The principal exceptions to this restriction are as follows:

a where the provision of personal data is required by laws and regulations;[33]

---

28 Article 18(1) APPI.

29 Article 19 APPI.

30 Article 21 APPI. For example during training sessions and monitoring whether employees comply with internal rules regarding personal information protection.

31 Article 22 APPI. The Economic and Industrial Guidelines say: 'The necessary and appropriate supervision includes that an entrustment contract contains the measures which are mutually agreed upon by both parties of entruster and trustee as necessary and appropriate measures regarding the handling of personal data, and that it is confirmed periodically in the predetermined time interval whether such measures are properly executed.' The Economic and Industrial Guidelines also mention the matters that are preferable to be contained in a contract when the handling of personal data is entrusted, such as clarification of the responsibilities of entruster and trustee, reporting in writing to an entruster when re-entrusting, and content and frequency of reporting regarding the status of handling personal data to an entruster, etc. (p. 49).

32 Article 23(1) APPI.

33 Article 23(1)(i) APPI. The Economic and Industrial Guidelines mention the following cases:

a submission of a payment record to the Director of the Taxation Office in accordance with Paragraph 1 of Article 225 of the Income Tax Law, etc.;

b response to the investigation of a subsidiary company by the auditors of a parent company in accordance with Paragraph 3 of Article 381 of the Company Law; and

b where a business operator handling personal information agrees to discontinue, at the request of the subject, providing such personal data as will lead to the identification of that person, and where the business operator, in advance, notifies the person of the following or makes such information readily available to the person:[34]
- the fact that the provision to a third party is the purpose of use;
- which items of personal data will be provided to a third party;
- the method of provision to a third party; and
- the fact that the provision of such personal data as might lead to the identification of the person to a third party will be discontinued at the request of the person;

c where a business operator handling personal information outsources the handling of personal data (for example, to service providers), in whole or in part, to a third party within the scope necessary for the achievement of the purpose of use;[35]

d where personal information is provided as a result of the takeover of business in a merger or other similar transaction;[36] and

e where personal data is used jointly between specific individuals or entities and where: (1) the facts, (2) the items of the personal data used jointly, (3) the scope of the joint users, (4) the purpose for which the personal data is used by them, and (5) the name of the individual or entity responsible for the management of the personal data concerned are notified in advance to the person or put in a readily accessible condition for the person.[37]

Public announcement of matters concerning retained personal data

Pursuant to Article 24(1) APPI, a business operator handling personal information must put the name of the business operator handling personal information and the purpose of use of all retained personal data in an accessible condition for the person (such a condition of accessibility includes cases in which a response is made without delay upon the request of the person).[38]

---

c response to an audit of financial statements pursuant to the provisions of Article 396 of the Company Law and Sub-article 2 of Article 193 of the Securities and Exchange Law.

34 Article 23(2) APPI.

35 Article 23(4)(i) APPI.

36 Article 23(4)(ii) APPI.

37 Article 23(4)(iii) APPI.

38 The Economic and Industrial Guidelines provide examples of what corresponds to such an accessible condition for the person, such as creating an enquiry counter and establishing a system so that a response to an enquiry is made verbally or in writing; ensuring placement of brochures in sales stores; and clearly describing the email address for enquiries in online electronic commerce.

Correction

When a business operator handling personal information is requested by a person to correct, add, or delete such retained personal data as may lead to the identification of the person on the ground that the retained personal data is incorrect, the business operator must make an investigation without delay within the scope necessary for the achievement of the purpose of use and, on the basis of the results, correct, add, or delete the retained personal data, except in cases where special procedures are prescribed by any other laws and regulations for such correction, addition or deletion.[39]

IV INTERNATIONAL DATA TRANSFER

There is no specific provision regarding international data transfers in the APPI. However, it is generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI would be applicable to the entity handling personal information in Japan. With some exceptions prescribed in the APPI (see Section III.ii, 'Restrictions on provision to a third party', *supra*), prior consent is required for the transfer of personal information to a third party.[40] The Economic and Industrial Guidelines provide examples of providing data to a third party pursuant to Article 23(1) APPI. Among these are the transfer of personal data between companies within the same group, including the exchange of personal data between a parent company and a subsidiary company, among fellow subsidiary companies and among group companies.

V COMPANY POLICIES AND PRACTICES

i Security control measures

A business operator handling personal information must take necessary and proper measures for the prevention of leakage, loss or damage of the personal data.[41] Control measures may be systemic, human, physical or technical. Examples of these are listed below.

Systemic security control measures[42]

a Preparing the organisation's structure to take security control measures for personal data;

39 Article 26(1) APPI.

40 Article 23(1) APPI.

41 Article 20 APPI.

42 2-2-3-2 [Security Control Measures (an issue related to Article 20 APPI)] (p. 32) of the Economic and Industrial Guidelines.

b preparing the regulations, and procedure manuals that provide security control measures for personal data and operating in accordance with the regulations and procedure manuals;[43]
c preparing the means by which the status of handling personal data can be looked through;
d assessing, reviewing and improving the security control measures for personal data; and
e responding to data security incidents or violations.

Human security control measures[44]

a Concluding a non-disclosure agreement with workers when signing the employment contract and concluding a non-disclosure agreement between an entruster and trustee in the entrustment contract, etc. (including the contract of supply of a temporary labourer).
b familiarising workers with internal regulations and procedures through education and training.

Physical security control measures[45]

a Implementing controls on entering and leaving a building or room where appropriate;
b preventing theft, etc.; and
c physically protecting equipment and devices.

Technical security control measures[46]

a Identification and authentication for access to personal data;
b control of access to personal data;
c management of authority to access personal data;
d recording access to personal data;
e countermeasures preventing unauthorised software on an information system handling personal data;
f measures when transferring and transmitting personal data;
g measures when confirming the operation of information systems handling personal data; and
h monitoring information systems that handle personal data.

43 The Economic and Industrial Guidelines provide in detail the preferable means of preparing regulations and procedure manuals (p. 31).

44 2-2-3-2 (p. 44) of the Economic and Industrial Guidelines.

45 2-2-3-2 (p. 45) of the Economic and Industrial Guidelines.

46 2-2-3-2 (p. 46) of the Economic and Industrial Guidelines.

VI DISCOVERY AND DISCLOSURE

i E-discovery

Japan does not have an e-discovery system equivalent to that in the United States. Electronic data that include personal information can be subjected to a judicial order of disclosure by a Japanese court during litigation.

ii Disclosure

When a business operator handling personal information is requested by a person to disclose such retained personal data as may lead to the identification of the person, the business operator must disclose the retained personal data without delay by a method prescribed by a Cabinet Order.[47] However, in the following circumstances, the business operator may keep all or part of the retained personal data undisclosed:[48]

a where disclosure is likely to harm the life, person, property, or other rights or interests of the person or a third party;

b where disclosure is likely to seriously impede the proper execution of the business of the business operator handling the personal information; or

c where disclosure violates other laws and regulations.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement and sanctions:

Enforcement agencies

The enforcement agencies in data protection matters are the Consumer Affairs Agency;[49] and ministries and agencies concerned with jurisdiction over the business of the relevant entities.[50]

47 The method specified by a Cabinet Order under Paragraph 1 of Article 25 APPI shall be the provision of documents (or 'the method agreed upon by the person requesting disclosure, if any'). Alternatively, according to the Economic and Industrial Guidelines, if the person who made a request for disclosure did not specify a method or make any specific objections, then they may be deemed to have agreed to whatever method the disclosing entity employes.

48 Article 25(1) APPI.

49 In Japan, there is no single central data protection authority. The Consumer Affairs Agency is the central authority in respect of the APPI in general.

50 The relevant entities are those entities (Entity Handling Personal Information) that have used a personal information database with details of over 5,000 individuals on any day in the past six months. (Article 2 of the Order for enforcement of the Act on the Protection of Personal Information (Cabinet Order 506, 2003, enacted on 10 December 2003).

Main penalties[51]

A business operator that violates orders issued under Paragraphs 2 or 3 of Article 34 (recommendations and orders by the competent minister in the event of a data security breach) shall be sentenced to imprisonment with forced labour of not more than six months or to a fine of not more than ¥300,000.[52]

A business operator that does not make a report[53] as required by Articles 32 or 46 or that has made a false report shall be sentenced to a fine of not more than ¥300,000 yen.[54]

ii Recent enforcement cases

Information breach at a computer company

An outsourcing contractor of a computer company had their customer information acquired by a criminal following an illegal intrusion into the company's network system. In May 2011, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the computer company reform its security control measures, supervision of outsourcing contractors and training for outsourcing contractors and employees (in respect of violation of the duty regarding supervision of an outsourcing contractor under Article 22[55] APPI).[56]

Information breach at a mobile phone company

The email addresses of a mobile phone company were reset and email addresses of the customers and the mail texts were disclosed to third parties. In January 2012, the Ministry of Internal Affairs and Communications (MIC) promulgated an administrative

51 The Unfair Competition Prevention Act (Act No. 47 of 1993) prohibits certain acts (Unfair Competition), including (1) an act to acquire a trade secret from the holder by theft, fraud or other wrongful methods; and (2) an act to use or disclose the trade secret so acquired. For the prevention of unfair competition, the Act provides measures, such as injunctions, claims for damages and penal provisions (imprisonment for a term not exceeding five years or a fine in an amount not exceeding ¥5 million. In the case of a juridical person, a fine not exceeding ¥300 million (in certain cases the fine is not to exceed ¥100 million) may be imposed (Articles 21 and 22).

52 Article 56 APPI.

53 The competent minister may have a business operator handling personal information make a report on the handling of personal information to the extent necessary for fulfilling the duties of a business operator (Articles 32 and 46 APPI).

54 Article 57 APPI.

55 See Section III.ii, 'Maintenance of the accuracy of data and supervision of employees or outsourcing contractors', *supra*.

56 www.meti.go.jp/english/press/2011/0527_04.html.

guidance requesting that the mobile phone company take the necessary measures to prevent a recurrence and to report the result to the Ministry (in respect of violation of the duty regarding security control measures under Article 20[57] APPI).[58]

Information theft from mobile phone companies

The manager and employees of an outsourcing contractor of three mobile phone companies acquired customer information from the mobile phone companies unlawfully through their customer information management system and disclosed the customer information to a third party. In November 2012, the MIC introduced an administrative guidance requesting that the mobile phone companies reform their security control measures, supervision of outsourcing contractors and training for outsourcing contractors and employees (in respect of violation of the duty regarding security control measures under Article 20 APPI and Article 11 of the MIC Guideline on Protection of Personal Information in Telecommunications.[59] There was also found to be a violation of the duty regarding the supervision of outsourcing contractors under Article 22 APPI and Article 12 of the above-mentioned MIC Guideline).[60]

Information theft from a mobile phone company

In July 2012, a former store manager of an agent company of a mobile phone company was arrested for disclosing customer information of the mobile phone company to a research company (in respect of violation of the Unfair Competition Prevention Act). The Nagoya District Court in November 2012 gave the defendant a sentence of one year and eight months' imprisonment with a four-year stay of execution and a fine of ¥1 million.[61]

Information theft from an educational company

In July 2014, it was revealed that the customer information of an educational company (Benesse Corporation) had been stolen and sold to third parties by employees of an outsourcing contractor of the educational company. In September 2014, the Ministry of Economy, Trade and Industry promulgated an administrative guidance requesting that the educational company reform its security control measures and supervision of outsourcing contractors (in respect of the violation of the duty regarding security control measures under Article 20 APPI. There was also found to be a violation of the duty regarding the supervision of an outsourcing contractor under Article 22 APPI).

---

57 See Section V.i, 'Security control measures' *supra*.

58 www.soumu.go.jp/menu_news/s-news/01kiban05_02000017.html (available only in Japanese).

59 Announcement No. 695 of 31 August 2004 by the MIC.

60 www.soumu.go.jp/menu_news/s-news/01kiban08_02000094.html (available only in Japanese).

61 Nikkei News website article on November 6 of 2012 (available only in Japanese): www.nikkei.com/article/DGXNASFD05015_V01C12A1CN8000/.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As stated in Section IV, *supra*, it is generally considered that when an entity handling personal information in Japan obtains personal information from business operators outside Japan or assigns personal information to business operators outside Japan, the APPI would be applicable to the entity handling personal information in Japan.

IX CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The amendments to the Criminal Code,[62] effective since 14 July 2011, were enacted to prevent and prosecute cybercrimes. Since under the previous law it was difficult to prosecute a person who merely stored a computer virus in his or her computer for the purpose of providing or distributing it to the computers of others, now, a person who not only actively creates, provides or distributes a computer virus, but also who acquires or stores a computer virus for the purpose of providing or distributing it to the computers of others without justification may be held criminally liable under the amendments.

Following the 2011 amendments, three primary types of behaviours are considered as cybercrimes: (1) the creation or provision of a computer virus; (2) the release of a computer virus; and (3) the acquisition or storage of a computer virus. Also, the Act on the Prohibition of Unauthorised Computer Access[63] (APUCA) was also amended on 31 March 2012 and took effect in May of that year. The APUCA identified additional criminal activities, such as the unlawful acquisition of a data subject's user ID or password for the purpose of unauthorised computer access, and the provision of a data subject's user ID or password to a third party without justification.

Following a 2004 review[64] the government has begun developing essential functions and frameworks aimed at addressing information security issues. For example, the National Information Security Centre was established on 25 April 2005 and the Information Security Policy Council was established under the aegis of an IT Strategic Headquarters (itself part of the Cabinet) on 30 May 2005.[65]

A bill on the Basic Law of Cybersecurity, which obliges all government ministries and agencies to report cyberattacks and aims to strengthen the authority of the National Information Security Centre, is being discussed in the Diet.

62 Act No. 45 of 1907, Amendment: Act No. 74 of 2011.

63 Act No. 128 of 199, Amendment: Act No. 12 of 2012.

64 Review of the Role and Functions of the Government in terms of Measures to Address Information Security Issues (IT Strategic Headquarters, 7 December 2004).

65 See 'Japanese Government's Efforts to Address Information Security Issues – Focusing on the Cabinet Secretariat's Efforts', NISC: www.nisc.go.jp/eng/pdf/overview_eng.pdf) and the government's international cybersecurity strategy: www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf.

ii Data security breach

There is no express provision in the APPI creating an obligation to notify data subjects or data authorities in the event of a data security breach. However, there are various guidelines issued by government ministries, some of which stipulate notifying the affected data subjects or governmental authorities promptly upon the occurrence of a data security breach.[66] In addition, the competent ministries have the authority to collect reports from, advise, instruct, or give orders to the data controllers.[67]

An organisation that is involved in a data breach may, depending on the circumstances, be subject to a suspension, closure or cancellation of the whole or part of its business operations, an administrative fine, penalty or sanction, civil actions and class actions or a criminal prosecution.

X OUTLOOK

i The revision of the APPI

As stated in Section II, *supra*, on 24 June 2014, the Japanese government published the Policy Outline of the Institutional Revision for Use of Personal Data, and the revised APPI legislation passed the Diet on 3 September 2015. The revised APPI will be in full force in 2017, but its effective date has not been set (as of this writing). This revision is the first major amendment to the APPI. A brief summary of the revision is given below.

ii Clarification of the definition of personal information

Under Article 2 APPI, 'personal information' is defined as the information about a living person that can identify him or her by name, date of birth or other description contained in such information (including information that will allow easy reference to other information that will enable the identification of the specific individual). Under the revised APPI, the following information is clarified as personal information:

a personal identifiable code, including, but not limited to, any code on physical characteristics of individuals (i.e., fingerprints) and individually allocated numbers (i.e., passport numbers and driver licence numbers); and

66 The Economic and Industrial Guidelines say it is preferable to apologise to the person for the accident or violation, and to contact the person as much as possible to prevent secondary damage except in certain instances, including where the personal data that was lost was immediately recovered without being seen by a third party, since it is conceivable that contacting the person can be omitted when the rights and interests of the person have not been infringed and it seems that there is no or extremely little likelihood of infringement. The Guidelines Targeting Financial Sector Pertaining to the Act on the Protection of Personal Information also mention the obligations that apply in the event of a data security breach.

67 Articles 32–34 APPI.

b sensitive personal information (i.e., race, creed, social status, medical history, criminal records, damage caused by a crime and the other information that may be designated by the Cabinet Order), the handling of which requires certain special measures.

iii Ensuring effective use of personal information

To ensure effective use of huge amounts of personal data (big data), the revised APPI provides that a business operator handling personal information may anonymise personal information and provide it to third parties without their consent to the extent that such treatment complies with regulations to be promulgated by the data protection authority newly created under the revised APPI.

iv Enhancement of the protection of personal information

The revised APPI:

a imposes obligations on a business operator handling personal information to verify third parties' names and how they obtained personal information when it receives personal information from those third parties;

b imposes obligations on a business operator handling personal information to keep accurate records for a certain period when it provides third parties with personal information; and

c establishes criminal liability for handling personal information with a view to making illegal profits.

v Establishment of the Personal Information Protection Commission

The revised APPI creates a new independent data protection authority, the Personal Information Protection Commission, which is authorised to address legal requirements and self-regulation matters.

vi Globalisation of personal information handling

The revised APPI introduces the following provisions on cross-border data transfers:

a personal data may not be transferred overseas without prior consent from the person except where a transferee foreign country is regarded by the Personal Information Protection Commission as having data protection standards equivalent to those of Japan; and

b the Personal Information Protection Commission may, under some circumstances, provide foreign enforcement authorities with useful information to assist their enforcement actions.

vii Other amendments

a The revised APPI requires that provision of personal information to third parties without consent be filed with the Personal Information Protection Commission.

b The revised APPI will be applied to business operators that have used any personal information database, regardless of the number of individuals whose personal information is involved.[68]

68 See footnote 3, *supra*.

Chapter 22

SINGAPORE

Yuet Ming Tham and Jillian Lee[1]

I OVERVIEW

The Personal Data Protection Act 2012 (PDPA) is Singapore's first comprehensive framework established to ensure the protection of personal data. The Bill was passed in 2012 but implementation was in phases so that organisations had 18 months to bring their activities into compliance with the PDPA. Provisions relating to the Do Not Call (DNC) Register came into force on 2 January 2014 whereas the substantive data protection provisions subsequently came into force on 2 July 2014. Under the Act, the Personal Data Protection Commission (PDPC) was set up to administer and enforce the Act.

Before the PDPA, data protection obligations were sector-specific and limited in scope. With a growing list of countries enacting similar laws, there was a strong need to bring Singapore's data protection regime on par with international standards and facilitate cross-border transfers of data. Indeed, Singapore sees the PDPA as an essential regime to 'enhance its competitiveness and strengthen our position as a trusted business hub',[2] necessary to achieving Singapore's aspirations of being a choice location for data hosting and management activities.

One notable feature of the PDPA is that government agencies do not fall within the ambit of the PDPA. The reason for this, as discussed in parliament, is that government agencies collect data where necessary to carry out their regulatory and statutory functions. In any event, the public sector is governed by similar data protection rules, some of which are even stricter that the PDPA.[3]

---

1 Yuet Ming Tham is a partner and Jillian Lee is an associate at Sidley Austin LLP.

2 Yaacob Ibrahim, Minister for Information, Communications and the Arts, in the Second Reading Speech on the Personal Data Protection Bill 2012.

3 Ibid.

In this chapter, we will outline the key aspects of the PDPA, which includes a brief discussion of the key concepts, the obligations imposed on data handlers, and the interplay between technology and the PDPA. Specific regulatory areas such as the protection of minors, financial institutions, employees and electronic marketing will also be considered. International data transfer is particularly pertinent in the increasingly connected world; how Singapore navigates between practical considerations and protection of the data will be briefly examined. We will also consider the enforcement of the PDPA in the event of non-compliance. In relation to cybersecurity, Singapore has recently beefed up its laws in this regard and recognised the potentially devastating effects in the event of a compromise or data breach. Finally, we will highlight future developments to keep a close eye on.

II THE YEAR IN REVIEW

There have been a large number of clarifications and updates to the PDPA and to its subsidiary legislation. Given the number of updates, a selection of the most significant of these is set out below.

On 23 January 2015, the Personal Data Protection (Appeal) Regulations 2015 (PDPAR) and the Personal Data Protection (Amendment of Seventh Schedule) came into effect. The PDPAR sets out the procedures for making appeals against the PDPC's decisions or directions[4] (e.g., appeals must be submitted within 28 days after the issuance of the PDPC's direction or decision). Companies that wish to make an appeal against the PDPC's decisions or directions are subject to the appeal procedure set out in the PDPAR (e.g., being required to prepare a notice of appeal, and being required to exercise their right of reply within a prescribed time).

On 8 May 2015, new Advisory Guidelines on Requiring Consent for Marketing Purposes (AGMP) were also issued by the PDPC.[5] As previously mentioned, these guidelines help organisations understand and comply with the PDPA. Sample clauses[6] for obtaining and withdrawing consent were also released by the PDPC. The AGMP provides that on obtaining consent under the DNC provisions, if an organisation wishes to send a 'specified message'[7] (as defined in Section 37 of the PDPA) to a Singapore telephone number, the DNC provisions will apply. The DNC provisions prohibit organisations from sending certain types of marketing messages (in the form of voice

4 Section 34(1) PDPA provides for an individual's or an organisation's right of appeal.

5 The revised guidelines issued are Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Advisory Guidelines on the Do Not Call Provisions, and Advisory Guidelines on the Personal Data Protection Act for Selected Topics.

6 https://www.pdpc.gov.sg/docs/default-source/Templates/sample-clauses-for-obtainin g-and-withdrawing-consent-(8-may-2015).pdf?sfvrsn=2.

7 A 'specified message' is defined in Section 37 of the PDPA to mean a message that achieves any one of the purposes listed under Section 37. This includes offering, promoting and advertising goods or services, business opportunities, and interest in land.

calls, text or fax messages) to Singapore telephone numbers registered with the DNC registry. The AGMP therefore provide greater clarity as to whether an organisation may require an individual to give his or her consent for marketing purposes under the PDPA.

Data analytics in Singapore have also improved, with the country having increasingly sophisticated software and more people trained to handle big data sets. One good example would be how Khoo Teck Puat Hospital has begun to apply analytics for the screening of obstructive sleep apnea.[8] The PDPC also published the Guide to Securing Personal Data in Electronic Medium on 8 May 2015. This guide seeks to provide recommendations on good practices that organisations should adopt to protect electronic personal data, The Guide on Managing Data Breaches was also published by the PDPC on 8 May 2015 to help organisations manage personal data breaches effectively.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The PDPA framework is built around the concepts of consent, purpose and reasonableness. The main concept may be summarised as follows: organisations may collect, use or disclose personal data only with the individual's knowledge and consent (subject to certain exceptions) for a purpose that would be considered appropriate to a reasonable person in the circumstances.

There is no prescribed list of 'personal data'; rather, it is defined broadly as data about an individual, whether or not it is true, who can be identified from that data or in conjunction with other information to which the organisation has or is likely to have access.[9]

Also, the PDPA does not distinguish between personal data in its different forms or mediums. Thus, there is no distinction made for personal data that is 'sensitive', or between data that is in electronic or hard copy formats. There are also no ownership rights conferred on personal data to individuals or organisations.[10]

There are certain exceptions to which the PDPA would apply. Business contact information of an individual generally falls outside the ambit of the PDPA,[11] as does

8 www.todayonline.com/singapore/big-data-making-great-difference-healthcare?page=1.

9 Section 2 of the PDPA.

10 Section 5.28, PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act, issued on 24 September 2013 and revised on 8 May 2015 (the PDPA Key Concepts Guidelines).

11 Section 4(5) of the PDPA.

personal data that is publicly available.[12] In addition, personal data of an individual who has been deceased for over 10 years[13] and personal data contained within records for over 100 years is exempt.[14]

Pursuant to the PDPA, organisations are responsible for personal data in their possession or under their control.[15] 'Organisations' include individuals who are resident in Singapore, local and foreign companies, associations, and bodies (incorporated and unincorporated) whether or not they have an office or a place of business in Singapore.[16] The PDPA does not apply to public agencies.[17] Individuals acting in a personal or domestic capacity, or where they are an employee acting in the course of employment within an organisation, are similarly excluded from the obligations imposed by the PDPA.[18]

Where an organisation acts in the capacity of a data intermediary, namely an organisation that processes data on another's behalf, it would only be subject to the protection and retention obligations under the PDPA. The organisation that engaged its services remains fully responsible in respect of the data as if it had processed the data on its own.[19]

There is no requirement to prove harm or injury to establish an offence under the PDPA, although this would be necessary in calculating damages or any other relief to be awarded to the individual in a private civil action against the non-compliant organisation.[20]

Subsidiary legislation to the PDPA includes implementing regulations relating to the DNC Registry,[21] enforcement,[22] composition of offences,[23] requests for access to and correction of personal data and the transfer of personal data outside Singapore.[24]

There is also various sector-specific legislation such as the Banking Act, the Telecommunications Act and the Private Hospitals and Medical Clinics Act, imposing specific data protection obligations. All organisations will have to comply with PDPA requirements in addition to the existing sector-specific requirements. In the event of any inconsistencies, the provisions of other laws will prevail.[25]

---

12 Second Schedule Paragraph 1(c); Third Schedule Paragraph 1(c); Fourth Schedule Paragraph 1(d) of the PDPA.

13 Section 4(4)(b) of the PDPA. The protection of personal data of individuals deceased for less than 10 years is limited; only obligations relating to disclosure and protection (Section 24) continue to apply.

14 Section 4(4) of the PDPA.

15 Section 11(2) of the PDPA.

16 Section 2 of the PDPA.

17 Section 4(1)(c) of the PDPA.

18 Section 4(1)(a) and (b) of the PDPA.

19 Section 4(3) of the PDPA.

20 Section 32 of the PDPA.

21 Personal Data Protection (Do Not Call Registry) Regulations 2013.

22 Personal Data Protection (Enforcement) Regulations 2014.

23 Personal Data Protection (Composition of Offences) Regulations 2013.

24 Personal Data Protection Regulations 2014.

25 Section 6 of the PDPA.

As mentioned in section I of this chapter, to ease organisations into the new data protection regime, the PDPC has released various advisory guidelines, as well as sector-specific advisory guidelines for the telecommunications, real estate agency, education, social services and healthcare sectors. The PDPC also published advisory guidelines on data protection as they relate to specific topics such as photography, analytics and research, data activities relating to minors and employment. While the advisory guidelines are not legally binding, they provide helpful insight and guidance into the problems particular to each sector or area.

ii General obligations for data handlers

The PDPA sets out nine key obligations in relation to how organisations collect, use and disclose personal data, as briefly described below:

Consent[26]

An organisation may only collect, use or disclose personal data for purposes to which an individual has consented. Where the individual provided the information voluntarily and it was reasonable in the circumstances, such consent may be presumed. Consent may be withdrawn at any time with reasonable notice. The provision of a service or product must not be made conditional upon the provision of consent beyond what is reasonable to provide that product or service.

An organisation may obtain personal data with the consent of the individual from a third part source under certain circumstances. For example, with organisations that operate in a group structure, it is possible for one organisation in the group to obtain consent to the collection, use and disclosure of an individual's personal data for the purposes of the other organisations within the corporate group.[27]

Purpose limitation[28]

Organisations are limited to collecting, using or disclosing personal data for purposes that a reasonable person would consider appropriate in the circumstances and for a purpose to which the individual has consented.

Notification[29]

Organisations are obliged to notify individuals of their purposes for the collection, use and disclosure of the personal data on or before such collection, use and disclosure. The PDPC has also released a Guide to Notification to assist organisations in providing clearer notifications to consumers on the collection, use and disclosure of personal data and includes suggestions on the layout, language and placement of notifications.[30]

26 Section 13 to 17 of the PDPA.

27 Para. 12.32, PDPA Key Concepts Guidelines.

28 Section 18 of the PDPA.

29 Section 20 of the PDPA.

30 PDPC Guide to Notification, issued on 11 September 2014.

Access and correction[31]

Save for certain exceptions, an organisation must, upon request, provide the individual with his or her personal data that the organisation has in its possession or control, and how the said personal data has been or may have been used or disclosed by the organisation during the past year. The organisation may charge a reasonable fee in responding to the access request.

The organisation is also obliged to allow an individual to correct an error or omission in his or her personal data upon request, unless the organisation is satisfied that there are reasonable grounds to deny such a request.[32]

An organisation should respond to an access or correction request within 30 days; beyond which the organisation should inform the individual in writing of the time they are able to provide a response to the request.[33]

Accuracy[34]

An organisation is obliged to make a reasonable effort to ensure that the personal data collected by or on behalf of the organisation is accurate and complete, if it is likely to be used to make a decision that affects an individual or is likely to be disclosed to another organisation.

Protection[35]

An organisation is obliged to implement reasonable and appropriate security safeguards to protect the personal data in its possession or under its control from unauthorised access or similar risks. As a matter of good practice, organisations are advised to design and organise their security arrangements in accordance with the nature and varying levels of sensitivity of such personal data.[36]

Retention limitation[37]

An organisation may not retain such personal data for longer than is reasonable for the purpose for which it was collected and no longer than is necessary in respect of its business or legal purpose. Beyond that retention period, organisations should either delete or anonymise their records.

31 Sections 21 and 22 of the PDPA.

32 Section 22(6) and Sixth Schedule of the PDPA.

33 Para. 15.34, PDPA Key Concepts Guidelines.

34 Section 23 of the PDPA.

35 Section 24 of the PDPA.

36 See discussion in Paragraphs 17.1–17.3, PDPC Key Concepts Guidelines.

37 Section 25 of the PDPA.

Transfer limitation[38]

An organisation may not transfer personal data to a country or territory outside Singapore, unless it has taken appropriate steps to ensure that the data protection provisions will be complied with, and that the overseas recipient is able to provide a standard of protection that is comparable to the protection under the PDPA (see Section IV, *infra*).

Openness[39]

An organisation is obliged to implement necessary policies and procedures in compliance with the PDPA, and ensure that such information is available publicly.

iii Technological innovation and privacy law

The PDPC considers that an IP address or network identifier such as an IMEI number, may not on its own be considered personal data as it simply identifies a particular networked device. However, where IP addresses are combined with other information such as cookies, individuals may be identified via their IP addresses, which would thus be considered personal data.

In relation to organisations collecting data points tied to a specific IP address, for example, to determine the number of unique visitors to a website, the PDPC takes the view that if the individual is not identifiable from the data collected, then such information collected would not be considered personal data. If, on the other hand, an organisation tracks a particular IP address and profiles the websites visited for a period such that the individual becomes identifiable, then the organisation would be found to have collected personal data.

Depending on the purpose for the use of cookies, the PDPA would apply only where cookies collect, use or disclose personal data. Thus, in respect of session cookies that only collect and store technical data, consent is not required.[40] Where cookies used for behavioural targeting involve the collection and use of personal data, the individual's consent is required.[41] Express consent may not be necessary in all cases; consent may be reflected when an individual has configured his or her browser setting to accept certain cookies but reject others.

If an organisation wishes to use cloud-based solutions that involve the transfer of personal data to another country, consent of the individual may be obtained pursuant to the organisation providing a written summary of the extent to which the transferred personal data will be protected to a standard comparable with the PDPA.[42] It is not clear how practicable this would be in practice; a cloud-computing service may adopt multi-tenancy and data commingling architectures to process data for multiple parties.

38 Section 26 of the PDPA.

39 Sections 11 and 12 of the PDPA.

40 Section 7.5–7.8, PDPC Advisory Guidelines on the Personal Data Protection Act for Selected Topics, issued 24 September 2013 and revised 11 September 2014 (the PDPA Selected Topics Guidelines).

41 Id., Paragraph 7.11.

42 Section 9(4)(a) of the Personal Data Protection Regulations 2014.

That said, organisations may take various precautions such as opting for cloud providers with the ability to isolate and identify the personal data for protection, and ensure it has established platforms with a robust security and governance framework.

As regards social media, one issue arises where personal data is disclosed on social networking platforms and becomes publicly available. As noted earlier, the collection, use and disclosure of publicly available data is exempt from the requirement to obtain consent. If, however, the individual changes his or her privacy settings so that the personal information is no longer publicly available, the PDPC has adopted the position that, as long as the personal data in question was publicly available at the point of collection, the organisation will be able to use and disclose the same without consent.[43]

iv Specific regulatory areas

Minors

The PDPA does not contain special protection for minors (under 21 years of age).[44] However, the Advisory Guidelines noted that a minor of 13 years or older typically has sufficient understanding to provide consent on his or her own behalf. Where a minor is below the age of 13, the organisation should obtain consent from the minor's parents or legal guardians on the minor's behalf.[45] The Education Guidelines[46] provide further guidance on when educational institutions seeking to collect, use or disclose personal data of minors are required to obtain the consent of the parent or legal guardian of the student.

Given the heightened sensitivity surrounding the treatment of minors, the PDPC recommends that organisations ought to take relevant precautions on this issue. Such precautions may include making the terms and conditions easy to understand for minors, placing additional safeguards in respect of personal data of minors and, where feasible, anonymising their personal data before use or disclosure.

Financial institutions

A series of notices issued by the Monetary Authority of Singapore (MAS)[47] provide that various financial institutions are required to:

a upon request, provide access as soon as reasonably practicable to personal data in the possession or under the control of the financial institution, which relates to an individual's factual identification data such as full name or alias, identification number, residential address, telephone number, date of birth and nationality; and

43 Para. 12.55, PDPA Key Concepts Guidelines.

44 Section 8.1, PDPA Selected Topics Guidelines.

45 Section 14(4) of the PDPA. See also discussion at Section 8.8 of the PDPA Selected Topics Guidelines.

46 Sections 2.5–2.8, PDPC Advisory Guidelines on the Education Sector, issued 11 September 2014.

47 MAS Notice SFA13-N01 regulating approved trustees; MAS Notice 626 regulating banks; MAS Notice SFA04-N02 regulating capital markets intermediaries; MAS Notice FAA-N06 regulating financial advisers; MAS Notice 824 regulating finance companies;

b correct an error or omission in relation to the categories of personal data set out above upon request by a customer if the financial institution is satisfied that the request is reasonable.

Also, legislative changes to the Monetary Authority of Singapore Act (the MAS Act), aimed at enhancing the effectiveness of the anti-money laundering and the countering of financing of terrorism (AML/CFT) regime of the financial industry in Singapore, came into force on 26 June 2015.

MAS will have the power to share information on financial institutions with its foreign counterparts under their home jurisdiction, on AML/CFT issues. MAS may also make AML/CFT supervisory enquiries on behalf of its foreign counterparts. Nonetheless, strong safeguards are in place to prevent abuse and 'fishing expeditions'. In granting requests for information, MAS will only provide assistance for *bona fide* requests. Any information shared will be proportionate to the specified purpose, and the foreign AML/CFT authority has to undertake not to use the information for any purpose other than the specified purpose, and to maintain confidentiality of any information obtained.

Electronic marketing

The PDPA contains provisions regarding the establishment of a national DNC Registry and obligations for organisations that send certain kinds of marketing messages to Singapore telephone numbers to comply with these provisions. The Healthcare Guidelines[48] provide further instructions on how the DNC provisions apply to that sector, particularly in relation to the marketing of drugs to patients. In relation to the DNC Register, the obligations only apply to senders of messages or calls to Singapore numbers, and where the sender is in Singapore when the messages or calls are made, or where the recipient accesses them in Singapore. Where there is a failure to comply with the DNC provisions, fines of up to S$10,000 may be imposed for each offence.

Employees

The PDPC provides that organisations should inform employees of the purposes of the collection, use and disclosure of their personal data and obtain their consent.

Employers are not required to obtain employee consent in certain instances. For instance, the collection of employee's personal data for the purpose of managing or terminating the employment relationship does not require the employee's consent although employers are still required to notify their employees of the purposes for its

MAS Notice 3001 regulating holders of money-changer's licences and remittance licences; MAS Notice PSOA-N02 regulating holders of stored value facilities; MAS Notice 314 regulating life insurers; MAS Notice 1014 regulating merchant banks; and MAS Notice TCA-N03 regulating trust companies.

48 Section 6 of the PDPC Advisory Guidelines for the Healthcare Sector, issued 11 September 2014.

collection, use and disclosure.[49] Examples of managing or terminating an employment relationship can include using the employee's bank account details to issue salaries or monitoring how the employee uses company computer network resources. The PDPA does not prescribe the manner in which employees may be notified of the purposes of the use of their personal data; as such, organisations may decide to inform their employees of these purposes via employment contracts, handbooks, or notices in the company intranet.

Also, employee personal data necessary for 'evaluative purposes' such as to determine the suitability of an individual for employment, neither requires the potential employee to consent to nor to be notified of its collection, use or disclosure.[50] Other legal obligations, such as to protect confidential information of their employees, will nevertheless continue to apply.[51]

Section 25 of the PDPA requires an organisation to cease to retain documents relating to the personal data of an employee once such retention is no longer necessary.

IV INTERNATIONAL DATA TRANSFER

An organisation may only transfer personal data outside Singapore subject to requirements prescribed under the PDPA so as to ensure that the transferred personal data is afforded a standard of protection comparable to the PDPA.[52]

An organisation may transfer personal data overseas if:

a it has taken appropriate steps to ensure that it will comply with the data protection provisions while the personal data remains in its possession or control; and

b it has taken appropriate steps to ensure that the recipient is bound by legally enforceable obligations to protect the personal data in accordance with standards comparable to the PDPA.[53] Such legally enforceable obligations would include any applicable laws of the country to which the personal data is transferred, contractual obligations or binding corporate rules for intra-company transfers.[54]

Notwithstanding the above, an organisation is taken to have satisfied the latter requirement if, *inter alia*, the individual consents to the transfer pursuant to the

49 Para. 1(o) Second Schedule, Para. 1(j) Third Schedule, and Para. 1(s) Fourth Schedule of the PDPA.

50 Para. 1(f) Second Schedule, Para. 1(f) Third Schedule and Para. 1(h) Fourth Schedule of the PDPA.

51 Sections 5.13 to 5.17 of the PDPA Selected Topics Guidelines.

52 Section 26(1) of the PDPA. The conditions for the transfer of personal data overseas are specified within the Personal Data Protection Regulations 2014.

53 Regulation 9 of the PDP Regulations.

54 Regulation 10 of the PDP Regulations.

organisation providing a summary in writing of the extent to which the personal data transferred to another country will be protected to a standard comparable to the PDPA;[55] or where the transfer is necessary for the performance of a contract.

In respect of personal data that simply passes through servers in Singapore en route to an overseas destination, the transferring organisation will be deemed to have complied with the transfer limitation obligation.[56]

The Advisory Guidelines on Key Concepts in the Personal Data Protection Act (AGKC)[57] also provide examples to illustrate situations in which organisations are deemed to have transferred personal data overseas in compliance with its transfer limitation obligation pursuant to Section 26 of the PDPA, regardless of whether the foreign jurisdiction's privacy laws are comparable to the PDPA. An example given is when a tour agency needs to share a customer's details (e.g., his or her name and passport number) to make hotel and flight bookings. The tour agency is deemed to have complied with Section 26 since the transfer is necessary for the performance of the contract between the agency and the customer.

An organisation is also deemed to have complied with the transfer limitation obligation if the transfer is necessary for the performance of a contract between a Singaporean company and a foreign business, and the contract is one that a reasonable person would consider to be in the individual's interest.

Other examples given by the AGKC include the transferring of publicly available personal data, and transferring a patient's medical records to another hospital where the disclosure is necessary to respond to a medical emergency.

The AGKC also sets out the scope of contractual clauses at Section 19.5 for recipients to comply with the required standard of protection in relation to personal data received so that it is comparable to the protection under the PDPA.

The AGKC sets out in a table (reproduced below) the areas of protection a transferring organisation should minimally set out in its contract in two situations: where the recipient is another organisation (except a data intermediary); and where the recipient is a data intermediary (i.e., an organisation which processes the personal data on behalf of the transferring organisation pursuant to a contract).

S/N	*Area of protection*	*Recipient*	
		Data intermediary	*Organisation (except data intermediary)*
1	Purpose of collection, use and disclosure by recipient		✓
2	Accuracy		✓
3	Protection	✓	✓
4	Retention limitation	✓	✓
5	Policies on personal data protection		✓

55 Regulation 9(3)(a) and 9(4)(a) of the PDP Regulations.

56 Regulation 9(2)(a) of the PDP Regulations.

57 Issued on 23 September 2013, and revised on 8 May 2015.

6	Access		✓
7	Correction		✓

V COMPANY POLICIES AND PRACTICES

Organisations are obliged to develop and implement policies and practices necessary to meet their obligations under the PDPA.[58] Organisations must also develop a complaints mechanism[59] and communicate to their staff the policies and practices they have implemented.[60] Information on policies and practices, including the complaints mechanism, is to be made available on request.[61] Every organisation is also obliged to appoint a data protection officer, who would be responsible for ensuring the organisation's compliance with the PDPA, and to make the data protection officer's business contact information publicly available.[62]

As a matter of best practice, an organisation should have in place notices and policies that are clear, easily accessible and comprehensible. Some of the policies and processes that an organisation may consider having in place are set out below.

i Data protection policy

If the organisation intends to collect personal data from individuals, it would be required to notify them of the purposes for the collection, use and disclosure of the personal data and seek consent before collecting the personal data. It should also state whether the personal data will be disclosed to third parties, and if so, who these organisations are. Further, where it is contemplated that the personal data may be transferred overseas, the organisation should disclose this and provide a summary of the extent to which the personal data would receive protection comparable to that under the PDPA, so that it may obtain consent from the individual for the transfer. The data protection policy may also specify how requests to access and correct the personal data may be made. To satisfy the requirement in the PDPA that data protection policies are available on request, the organisation may wish to make its policy available online.

ii Cookie policy

If the corporate website requires collection of personal data or uses cookies that require collection of personal data, users ought to be notified of the purpose for the collection, use or disclosure of the personal data, and prompted for their consent in that regard.

58 Section 12 (a) of the PDPA.

59 Section 12(b) of the PDPA.

60 Section 12(c) of the PDPA.

61 Section 12(d) of the PDPA.

62 Section 11(4) of the PDPA.

iii Complaints mechanism

The organisation should develop a process to receive and respond to complaints it receives, and this should be made available to the public.

iv Contracts with data intermediaries

Contracts with data intermediaries should set out clearly the intermediaries' obligations and include clauses relating to the retention period of the data and subsequent deletion or destruction, security arrangements, access and correction procedures, and audit rights of the organisation over the data intermediaries. Where a third party is engaged to collect data on its behalf, the contract should specify that the collection is conducted in compliance with the data protection provisions.

v Employee data protection policy

Employees should be notified of how their personal data may be collected, used or disclosed. The mode of notification is not prescribed, and the employer may choose to inform the employee of these purposes via employment contracts, handbooks, or notices on the company intranet. Consent is not required if the purpose is to manage or terminate the employment relationship, so for example, the company should notify employees that it may monitor network activities including company emails in the event of an audit or review.

vi Retention and security of personal data

Organisations should ensure that there are policies and processes in place to ensure that personal data is not kept longer than is necessary, and that there are adequate security measures in place to safeguard the personal data. An incident-response plan should also be created to ensure prompt responses to security breaches.

VI DISCOVERY AND DISCLOSURE

The data protection provisions under the PDPA do not affect any rights or obligations under other laws.[63] As such, where the law mandates disclosure of information that may include personal data, another law would prevail to the extent it is inconsistent with the PDPA. For instance, the Prevention of Corruption Act imposes a legal duty on a person to disclose any information requested by the authorities. Under those circumstances, the legal obligation to disclose information would prevail over the Data Protection provisions.

The PDPA has carved out specific exceptions in respect of investigations and proceedings. Thus, an organisation may collect data about an individual without his or her consent where such collection is necessary for any investigation or proceedings, so as not to compromise the availability or accuracy of the personal data.[64] Further, an organisation may use personal data about an individual without the consent of

63 Section 4(6) of the PDPA.

64 Second Schedule, Section 1(e) of the PDPA.

the individual if such use is necessary for any investigation or proceedings.[65] These exceptions, however, do not extend to internal audits or investigations. Nevertheless, it may be argued that consent from the employees are not required as such audits would fall within the purpose of managing or terminating the relationship.[66] Employees may be notified of such potential purposes of use of their personal data in their employee handbooks or contracts, as the case may be.

On an international scale, Singapore is active in providing legal assistance and sharing of information, particularly in respect of criminal matters. That said, the PDPC may not share any information with a foreign data protection body unless there is an undertaking in writing that it will comply with its terms in respect of the disclosed data. This obligation is mutual and the PDPA also authorises the PDPC to enter into a similar undertaking required for a foreign data protection body where required.[67]

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The PDPC is the key agency responsible for administering and enforcing the PDPA. Its role includes, among other things, reviewing complaints from individuals,[68] carrying out investigations (whether on its on accord or upon a complaint), prosecuting and adjudicating on certain matters arising out of the PDPA.[69]

To enable the PDPC to carry out its functions effectively, it has been entrusted with broad powers of investigation,[70] including the power to require organisations to produce documents or information and the power to enter premises with or without a warrant to carry out a search. In certain circumstances, the PDPC may obtain a search and seizure order from the state courts to search the premises and take possession of any material that appears to be relevant to the investigation.

Where the PDPC is satisfied that there is non-compliance with the data protection provisions, it may issue directions to the infringing organisation to rectify the breach, and impose financial penalties up to S$1 million.[71] The PDPC may also in its discretion compound the offence.[72] Certain breaches can attract penalties of up to three years' imprisonment.[73] In addition to corporate liability, the PDPA may also hold an officer of

65 Third Schedule, Section 1(e) of the PDPA.

66 As discussed earlier, consent is not required if the purpose for the collection, use and disclosure of personal data is for managing or terminating the employment relationship.

67 Section 10(4) of the PDPA.

68 Section 28 of the PDPA.

69 See Sections 28(2) and 29(1) of the PDPA. The PDPC has the power to give directions in relation to review applications made by complainants and contraventions to Parts III to VI of the PDPA.

70 Section 50 of the PDPA. See also Ninth Schedule of the PDPA.

71 Section 29 of the PDPA.

72 Section 55 of the PDPA.

73 Section 56 of the PDPA.

the company to be individually accountable if the offence was committed with his or her consent or connivance, or is attributable to his or her neglect.[74] Further, employers are deemed to be vicariously liable for the acts of their employees, unless there is evidence showing that the employer had taken steps to prevent the employee from engaging in the infringing acts.[75]

Directions issued by the PDPC may be appealed to be heard before the Appeal Committee. Thereafter, any appeals against decision of the Appeal Committee shall lie to the High Court, but only on a point of law or the quantum of the financial penalty. There would be a further right of appeal from the High Court's decisions to the Court of Appeal, as in the case of the exercise of its original civil jurisdiction.[76]

In relation to breaches of the DNC Registry provisions, the organisation may be liable for fines of up to S$10,000 for each breach.

ii Recent enforcement cases

As the provisions of the PDPA have only recently come into force, there has only been one enforcement case brought before the Singapore state courts. On 4 June 2014, the PDPC brought charges against a tuition agency and its director for 37 counts of contravening the DNC provisions relating to the organisation's obligation to check the DNC Registry before sending telemarketing messages. The defendants pleaded guilty to 13 of the 37 counts and were fined a total of S$80,000 by the state courts.

However, from the time the DNC provisions came into effect, on 2 January 2014, up to 23 May 2014, the PDPC has conducted investigations into 3,700 valid complaints from members of the public against 630 organisations, from sectors such as property, tuition and insurance.[77] Two organisations have had their offences compounded for amounts between S$500 and S$1,000. About 380 organisations that had received isolated complaints were issued warning notices regarding the sending of unsolicited telemarketing messages. There are no statistics available for the period up to May 2015.

iii Private litigation

Anyone who has suffered loss or damage directly arising from a contravention of the data protection provisions may obtain an injunction, declaration, damages or any other relief against the errant organisation in civil proceedings in court. However, no private action against the organisation may be taken until after the right of appeal has been exhausted and the final decision is made.[78]

74 Section 52 of the PDPA.

75 Section 53 of the PDPA.

76 Section 35 of the PDPA.

77 www.pdpc.gov.sg/docs/default-source/media/media-release---pdpc-takes-action-against-tuition-agency-and-organisations-(230514).pdf?sfvrsn=2.

78 Section 32 of the PDPA.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The PDPA applies to foreign organisations in respect of activities relating to the collection, use and disclosure of personal data in Singapore regardless of their physical presence in Singapore.

Thus, where foreign organisations transfer personal data into Singapore, the data protection provisions would apply in respect of activities involving personal data in Singapore. These obligations imposed under the PDPA may be in addition to any applicable laws in respect of the data activities involving personal data transferred overseas.

IX CYBERSECURITY AND DATA BREACHES

i Data breaches

While the PDPA obliges organisations to protect personal data, there is no requirement to notify authorities in the event of a data breach. There are, however, industry specific guidelines and notices that have imposed such reporting obligations. In that regard, the Monetary Authority of Singapore (MAS) has issued a set of notices to financial institutions on 1 July 2014 to direct that all security breaches should be reported to the MAS within one hour of discovery of the incident.

ii Cybersecurity

Singapore is not a signatory to the Council of Europe's Convention on Cybercrime. In Singapore, the Computer Misuse and Cybersecurity Act (the Cybersecurity Act) is the key legislation governing cybercrime and cybersecurity. In particular, it regulates:

a unauthorised access to or modification of computer material;[79]

b unauthorised use or interception of a computer service;[80] and

c unauthorised disclosure of access codes.[81]

The Cybersecurity Act was amended in 2013 to address cyberthreats to critical information infrastructure, namely systems necessary for the delivery of essential services to the public in key sectors.[82] In particular, the Minister of Home Affairs may direct entities to take such pre-emptive measures as necessary to prevent, detect or counter any cybersecurity threat posed to the national security, essential services or defence of Singapore or foreign relations of Singapore.[83]

79 Sections 3 and 5 of the Computer Misuse and Cybersecurity Act 2013.

80 Section 6 of the Computer Misuse and Cybersecurity Act 2013.

81 Section 8 of the Computer Misuse and Cybersecurity Act 2013.

82 This would include the energy, finance and banking, ICT, security and emergency services, transportation, water, government and healthcare sectors.

83 Section 15A of the Computer Misuse and Cybersecurity Act 2013.

X OUTLOOK

With the issuance of more guidelines, we expect to see a higher level of compliance and control in Singapore's data privacy and cybersecurity scene. The conscious effort made by the Singapore government to address the need to help organisations enhance IT security, especially for small and medium-sized enterprises, is also something that is apparent from the new developments. It is also likely that Singapore will see more industry-led guidelines.

It is anticipated that the government will continue to place more emphasis on developing Singapore's cybersecurity framework and focus on the protection of networks from cybersecurity attacks.

Finally, we can expect further collaboration between the government, the private sector and trade associations to promote and strengthen Singapore's cybersecurity and data protection regime.

Chapter 26

UNITED KINGDOM

William RM Long and Géraldine Scali[1]

I OVERVIEW

Like other countries in Europe, the United Kingdom has adopted an omnibus data protection regime implementing the EU Data Protection Directive 95/46/EC (the Data Protection Directive),[2] which regulates the collection and processing of personal data across all sectors of the economy.

II THE YEAR IN REVIEW

Recent developments in UK data protection law include the commencement in March 2015 of Section 56 of the UK Data Protection Act 1998 (DPA) making it a criminal offence to pressure an individual to make a request for his or her own personal information.

Also, in May 2015 the English Court of Appeal issued a landmark judgment against Google, which could open the door to privacy litigation in the United Kingdom.[3] The case concerned the collection by Google of Safari users' browser information, allegedly without their knowledge or consent. In its opinion, the Court of Appeal held that four individuals who used Safari browsers can bring a claim for breach of privacy and that the damages claimed can include distress – even in circumstances where there

1 William RM Long is a partner and Géraldine Scali is a senior associate at Sidley Austin LLP.

2 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 *Google Inc v. Vidal-Hall* [2015] EWCA Civ.

is no financial loss, as this had been the intention of the EU's Data Protection Directive. On 28 July, the UK Supreme Court granted Google Inc the permission to appeal part of the lower court ruling.[4]

In addition, over the past few months, the ICO updated its CCTV code of practice and also published search-result delisting criteria following the ruling by the Court of Justice of the European Union[5] that individuals can, in some cases, ask internet search providers to delete search results that contain information about them.[6]

Finally, in July 2015, only one year after the Data Retention and Investigatory Powers Act 2014 (the DRIP Act) received Royal Assent (see Section III.i, *infra*), the English High Court issued a judgment declaring the Act, which provides key surveillance authority for law enforcement and intelligence authorities, to be unlawful as it was determined that a number of the provisions were incompatible with EU human rights laws.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Privacy and data protection laws and regulations

In the United Kingdom, data protection is mainly governed by the Data Protection Act 1998 (DPA), which has implemented the Data Protection Directive into national law and entered into force on 1 March 2000.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications (EC Directive) (Amendments) Regulations 2011) (PECR) regulate direct marketing but also the processing of location and traffic data and the use of cookies and similar technologies. The PECR have implemented Directive 2002/58/EC[7] (as amended by Directive 2009/136/EC).

---

4 Google applied for an appeal to the Supreme Court on the following grounds: (1) whether the Court of Appeal was right to hold that claimant's claims for misuse of private information are tort claims for the purposes of the rules relating to service of the proceedings out of the jurisdiction; (2) whether the Court of Appeal was right to hold that Section 13(2) of the UK Data Protection Act 1998 was incompatible with Article 23 of the Data Protection Directive; and (3) whether the Court of Appeal was right to decline the application of Section 13(2) of the UK Data Protection Act 1998 on the grounds that it conflicts with the rights guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights. The Supreme Court gave permission to appeal only on points (2) and (3), and considered that point (1) did not raise an arguable point of law.

5 Case C-131/12 *Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014].

6 The criteria can be found at https://ico.org.uk/for-organisations/search-result-delisting-criteria/.

7 Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Key definitions under the DPA

a Data controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed;[8]

b data processor: any person (other than the employee of a data controller) who processes the data on behalf of the data controller;[9]

c data subject: an individual who is the subject of personal data;[10]

d personal data: data that relates to a living individual who can be identified from that data, or from that data and other information that is in the possession of, or is likely to come into the possession of, the data controller;[11]

e processing (in relation to information): obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including organisation, adaptation or alteration of the information or data; retrieval, consultation or use of the information or data, disclosure of the information of data by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data;[12] and

f sensitive personal data: personal data consisting of information as to the racial or ethnic origin of the data subject, his or her political opinions, his or her religious beliefs or information of a similar nature, whether the subject is a member of a trade union, his or her physical or mental health or condition, sexual life, the commission or alleged commission by him or her of any offence, or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any court in such proceedings.[13]

Data protection authority

The DPA and PECR are enforced by the ICO. The ICO also enforces and oversees the Freedom of Information Act 2000, which provides public access to information held by public authorities.[14] The ICO has independent status and is responsible for maintaining the public register of data controllers; promoting good practice by giving advice and guidance on data protection and working with organisations to improve the way they process data through audits, arranging advisory visits, and data protection workshops; ruling on complaints; and taking regulatory actions.

8 Section 1 DPA.

9 Ibid.

10 Ibid.

11 Ibid.

12 Ibid.

13 Section 2 DPA.

14 Freedom of Information Act 2000.

ii General obligations for data handlers

Under the DPA, data controllers must comply with the eight data protection principles[15] and ensuing obligations.

First principle: fair and lawful processing

Personal data must be processed fairly and lawfully. This essentially means that the data controller must: (1) have a legitimate ground for processing the personal data; (2) not use data in ways that have an unjustified adverse effect on the individuals concerned; (3) be transparent about how the data controller intends to use the personal data, and give the data subject appropriate privacy notices when collecting their personal data; (4) handle a data subject's personal data only in ways they would reasonably expect and consistent with the purposes identified to the data subject; and (5) make sure that nothing unlawful is done with the data.

Legal basis to process personal data

As part of fair and lawful processing, the processing must be justified by at least one of six specified grounds listed in Schedule 2 to the DPA.

The DPA applies a stricter regime in the case of sensitive personal data,[16] which may only be processed on the basis of certain limited grounds, including where the data controller has obtained the explicit consent of the data subject.[17]

Registration with the ICO

Under the DPA, a data controller processing personal data must make a notification to the ICO,[18] unless certain limited exemptions apply. A data controller who is not established in the United Kingdom, or any other European Economic Area (EEA) state, but is using equipment in the United Kingdom for processing personal data other than merely for the purposes of transit in the United Kingdom, has to appoint a representative in the United Kingdom and provide the contact name and details of the representative to the ICO in the registration form. Notification of the ICO consists of filling in a form and the payment of a fee, which must be paid when the data controller registers for the first time and then every year when the registration is renewed.

Data protection officer

There is no current legal requirement to appoint a data protection officer.

Information notices

Data controllers must provide data subjects with information on how their personal data is being processed. In general terms, an information notice should, according to the

15 Schedule 1 to the DPA.

16 See definition at Section III.i, *supra*.

17 Schedule 3 to the DPA.

18 Section 18 DPA.

ICO,[19] state: (1) the data controller's identity and, if the data controller is not based in the United Kingdom, the identity of its nominated UK representative; (2) the purposes for which the processing of personal data is intended; and (3) any additional information the data controller needs to give individuals in the circumstances to be able to process the data fairly.[20]

Second principle: processing for specified and lawful purposes

Personal data can only be obtained for one or more specified and lawful purposes, and must not be processed in a way that is incompatible with those purposes.

Third principle: personal data must be adequate, relevant and not excessive

A data controller must ensure that it holds sufficient personal data to fulfil its intended lawful purposes, but that personal data must be relevant and not excessive to those purposes.

Fourth principle: personal data must be accurate and kept up to date

Data controllers must ensure that personal data is accurate and, where necessary, kept up to date. The ICO recommends[21] data controllers to take reasonable steps to ensure the accuracy of any personal data obtained, ensure that the source of any personal data is clear, and carefully consider any challenges to the accuracy of information and whether it is necessary to update the information.

Fifth principle: personal data must not be kept for longer than necessary

Personal data processed for particular purposes should not be kept for longer than is necessary for those purposes. In practice, this means that the data controller must review the length of time it keeps personal data and consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain this information. Data controllers must also securely delete personal data that is no longer needed for this purpose or these purposes and update, archive or securely delete information if it goes out of date.

It is good practice to establish standard retention periods for different categories of information (e.g., employees' data and customer data). To determine the retention period for each category of information, data controllers should take into account and consider any legal or regulatory requirements or professional rules that would apply.[22]

Sixth principle: personal data must be processed in accordance with the rights of data subjects

Personal data should be processed in accordance with the rights of data subjects under the DPA. In particular, the data controller must: (1) provide information in response to

19 ICO, Privacy Notices Code of Practice, December 2010.

20 ICO, Guide to Data Protection, Part B 1, paragraph 25.

21 ICO, Guide to Data Protection.

22 Ibid.

a data subject's access request;[23] (2) comply with a justified request to prevent processing that is causing or will be likely to cause unwarranted damage or distress to the data subject or another person; (3) comply with a notice to prevent processing for the purposes of direct marketing; and (4) comply with a notice objecting to the taking of automated decisions.

Seventh principle: measures must be taken against unauthorised or unlawful processing of personal data

Appropriate technical and organisational measures must be taken by the data controller against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, the personal data. Where a data controller uses a data processor to process personal data on its behalf then the data controller must ensure that it has entered into a written contract that obliges the data processor to process only the personal data on the instructions of the data controller and to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

Eighth principle: transfers of personal data to a country or territory outside the European Economic Area

See Section IV, *infra*.

iii Technological innovation and privacy law

Anonymisation

The DPA does not apply to anonymous data. However, there has been a lot of discussion over when data is anonymous and the methods that could be applied to anonymise data.

The ICO in its guidance on anonymisation[24] recommends organisations using anonymisation to have in place an effective and comprehensive governance structure that should include: (1) a senior information risk owner with the technical and legal understanding to manage the process; (2) staff trained to have a clear understanding of anonymisation techniques, the risks involved and the means to mitigate them; (3) procedures for identifying cases where anonymisation may be problematic or difficult to achieve in practice; (4) knowledge management regarding any new guidance or case law that clarifies the legal framework surrounding anonymisation; (5) a joint approach with other organisations in the same sector or those doing similar work; (6) use of a privacy impact assessment; (7) clear information on the organisation's approach on anonymisation including how personal data is anonymised and the purpose of the anonymisation, the techniques used and whether or not the individual has a choice over the anonymisation of his or her personal data; (8) a review of the consequences of the anonymisation programme; and (9) a disaster-recovery procedure should re-identification take place and the individual privacy is compromised.

23 ICO, Subject Access Code of Practice.

24 In November 2012, the ICO published a code of practice on managing data protection risks related to anonymisation. This code provides a framework for organisations considering using anonymisation and explains what it expects from organisations using such processes.

Big data

The DPA does not prohibit the use of big data and analytics. However, because it raises various data protection issues, the ICO issued guidance in July 2014[25] considering data protection issues raised by big data. The ICO suggests how data controllers can comply with the DPA while using big data, covering a broad range of topics including anonymisation, privacy impact assessments, repurposing data, data minimisation, transparency and subject access. The guidance included three questions on which the ICO invited feedback. A summary of feedback on big data and data protection and the ICO position was published in April 2015.[26]

'Bring your own device' (BYOD)

The ICO has published guidance for companies on implementing BYOD[27] programmes allowing employees to connect their own devices to company IT systems. Organisations using BYOD should have a clear BYOD policy so that employees connecting their devices to the company IT systems clearly understand their responsibilities.

To address the data protection and security breach risks linked to BYOD, the ICO recommends that companies take various measures including considering which type of corporate data can be processed on personal devices; how to encrypt and secure access to the corporate data; how the corporate data should be stored on the personal devices; how and when the corporate data should be deleted from the personal devices; and how the data should be transferred from the personal device to the company servers.

Organisations should also install antivirus software on personal devices, provide technical support to the employees on their personal devices when they are used for business purposes and have in place a 'BYOD acceptable-use policy' providing guidance to users on how they can use their own devices to process corporate data and personal data.

Cloud computing

The use of cloud computing and how it complies with EU data protection requirements has been a subject of much discussion recently. The ICO, like many other data protection authorities in the EU, has published guidance on cloud computing.[28]

Cloud customers should choose their cloud provider based on economic, legal and technical considerations. According to the ICO it is important that at the very least such contracts allow cloud customers to retain sufficient control over the data to fulfil their data protection obligations.

The ICO proposes a checklist that organisations can follow prior to entering into an agreement with a cloud provider, with questions on confidentiality, integrity, availability and other legal and data protection issues.[29]

---

25 ICO, Guidelines on Big Data and Data Protection, 28 July 2014.

26 ICO, Summary of Feedback on Big Data and Data Protection and ICO Response, 10 April 2015.

27 ICO, Guidelines on Bring Your Own Device (BYOD), 2013.

28 ICO, Guidance on the Use of Cloud Computing, 2012.

29 See European Union Overview chapter for more details on cloud computing.

Cookies and similar technologies

In 2009, the e-Privacy Directive 2002/58/EC was amended.[30] This included a change to Article 5(3) of the e-Privacy Directive requiring consent for the use of cookies and similar technologies. This new requirement was implemented in the United Kingdom through the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011. As a result, organisations now have an obligation to obtain consent of website users to place cookies or similar technologies on their computers and mobile devices.[31] The consent obligation does not apply where the cookie is used 'for the sole purpose of carrying out the transmission of a communication over an electronic communication network' or is 'strictly necessary' to provide the service explicitly requested by the user. This exemption is applied restrictively and so could not be used when using analytical cookies. Organisations must also provide users with clear and comprehensive information about the purposes for which the information, such as that collected through cookies, is used.

The ICO has published guidance on the use of cookies, and provides recommendations on how to comply with the requirements and how to obtain consent. The ICO considers that implied opt-in consent is a valid form of consent if the consenting individual has taken some action from which the consent can be inferred, such as visiting the website and going from one page to another by clicking on a particular button.[32]

Since October 2012, the ICO has written to 291 organisations in relation to their compliance with the cookie rules following concerns raised by consumers.

iv Specific regulatory areas

Employee data

There is no specific law regulating the processing of employee data. However, the ICO has published an employment practices code and supplementary guidance to help organisations comply with the DPA and to adopt good practice.[33]

The code contains four parts covering: (1) recruitment and selection, providing recommendations with regards to the recruitment process and pre-employment vetting; (2) employment records, which is about collecting, storing, disclosing and deleting employees' records; (3) monitoring at work, which covers the employer's monitoring of employees' use of telephones, internet, email systems and vehicles and; (4) workers' health, covering occupational health, medical testing and drug screening.

30 Directive 2009/136/EC.

31 PECR Regulation 6.

32 ICO, Guidance on the Rules on Use of Cookies and Similar Technologies, 2012.

33 ICO, The Employment Practices Code – Supplementary Guidance, 2011.

Employee monitoring[34]

The DPA does not prevent employers monitoring their employees. However, monitoring employees will usually be intrusive and workers have legitimate expectations that they can keep their personal lives private. Workers are also entitled to a degree of privacy in their work environment.

Organisations should carry out a privacy impact assessment before starting to monitor their employees to clearly identify the purposes of monitoring, the benefit it is likely to deliver, the potential adverse impact of the monitoring arrangement, and to judge if monitoring is justified as well as take into account the obligation that arises from monitoring. Organisations should also inform workers who are subject to the monitoring of the nature, extent and reasons for monitoring unless covert monitoring is justified.

Employers should also establish a policy on use by employees of electronic communications explaining acceptable use of internet, phones and mobile devices, and the purpose and extent of electronic monitoring. It should also be outlined how the policy is enforced and the penalties for a breach of the policy.

Opening personal emails should be avoided where possible and should only occur where the reason is sufficient to justify the degree of intrusion involved.

Whistle-blowing hotlines

Under the DPA, the use of whistle-blowing hotlines (where employees and other individuals can report misconduct or wrongdoing) is permitted and their use is not restricted by the ICO. There is no specific UK guidance on the use of whistle-blowing hotlines. However, organisations using them in the United Kingdom will have to comply with the data-protection principles under the DPA.[35]

Electronic marketing[36]

Under the PECR, unsolicited electronic communication to individuals should only be sent with the recipient's consent.[37] The only exemption to this rule is known as 'soft opt-in', which will apply if the sender has obtained the individual's details in the course of a sale or negotiations for a sale of a product or service; the messages are only marketing for similar products; and the person is given a simple opportunity to refuse marketing when their details are collected, and if they do not opt out, they are given a simple way to do so in future messages. These UK rules on consent do not apply to marketing emails sent to companies and other corporate bodies.[38]

---

34 Ibid.

35 For guidance on how to comply with data protection principles under the DPA see WP 117 – Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes in the fields of accounting internal accounting controls, auditing matters, fight against bribery, banking and financial crime adopted on 1 February 2006.

36 ICO, Guide to the Privacy and Electronic Communications Regulations, 2013, and Direct Marketing Guidance, 2013.

37 PECR Regulation 22(2).

38 ICO, Direct Marketing Guidance, 2013.

Senders of electronic marketing messages must provide the recipients with the sender's name and a valid contact address.[39]

The ICO has created a direct-marketing checklist, which enables organisations to check if their marketing messages comply with the law and which also proposes a guide to the different rules on marketing calls, texts, emails, faxes and mail. The ICO has also published guidance on direct marketing.[40]

Financial services

Financial services organisations, in addition to data protection requirements under the DPA, also have legal and regulatory responsibilities to safeguard consumer data under the rules of the Financial Conduct Authority (FCA), which include having adequate systems and controls in place to discharge their responsibilities.

This includes financial services firms taking reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime, such as by misuse of customer data.[41]

Failure to comply with these security requirements may lead to the imposition of significant financial penalties by the FCA.

IV INTERNATIONAL DATA TRANSFER

Under the eighth principle of the DPA, personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.[42] The DPA provides various exemptions to permit transfers of personal data from the EEA to countries outside the EEA that do not provide an adequate level of protection, including:

a Consent – with the consent of the data subject, although as the ICO comments, valid consent means the data subject must have a real opportunity to withhold consent without inferring a penalty, or to subsequently withdraw consent. As a result, consent is unlikely to provide an adequate long-term framework in cases of repeated or structured transfer.

b Safe Harbor – where the company in the United States receiving the personal data is self-certified under the US Safe Harbor scheme organised by the US Department of Commerce, which exists for transfers of personal data from the EEA and from Switzerland. However, this was in October 2015 declared invalid by the Court of Justice of the European Union (CJEU). The status of Safe Harbor version 2.0 is still unknown, albeit negotiations between US authorities and the European Commission are ongoing.

39 PECR Regulation 23.

40 ICO, Direct Marketing Guidance, 2013.

41 SYSC 3.

42 Schedule 1 to the DPA.

c EU Model Contract Clauses – where the EU's standard contractual clauses (model contracts) for the transfer of personal data from a data exporter in the EEA to a data importer outside the EEA are entered into.

d Binding corporate rules – where the data controller has entered into binding corporate rules. As the lead data protection authority, the ICO has approved the binding corporate rules of 21 organisations so far.[43]

e Adequacy assessment – where in the view of the data controller there is an adequate level of protection for the personal data to be transferred; this requires an assessment of the circumstances of the transfer (such as the nature of the data, the purposes of the transfer, security measures taken etc.) and an assessment of the law in force in the country where the data is to be transferred.

f Other exceptions under the DPA – (1) where it is necessary for carrying out certain types of contract or if the transfer is necessary to set up the contract; (2) where it is necessary for reasons of substantial public interest (e.g., preventing and detecting crime, national security and collecting tax); (3) where it is necessary for the protection of the vital interests of the individual (e.g., matters of life and death); (4) where the personal data is part of a public register, as long as the person to whom the data is transferred complies with any restrictions on access to, or use of, the information in the register; and (5) where it is necessary in connection with legal proceedings (including future proceedings not yet under way), to get legal advice or where exercising or defending legal rights.

V DISCOVERY AND DISCLOSURE

The ICO has not published any specific guidance on this topic. E-discovery procedures and the disclosure of information to foreign enforcement agencies will, most of the time, involve the processing of personal data. As a result, organisations will have to comply with the data protection principles under the DPA in relation to e-discovery.

In practice this will mean informing data subjects about the processing of their personal data for this purpose. Organisations will also have to have a legal basis for processing the data. In the United Kingdom, companies may be able to rely on the legitimate-interest basis to disclose personal data unless the data contains sensitive data, in which case consent of the data subject will have to be obtained, or where the processing is necessary for the purposes of establishing, exercising or defending legal rights.[44]

A data transfer solution will also have to be implemented if the data is sent to a country outside the EEA that is not deemed to provide an adequate level of protection as discussed in Section IV, *supra*.

43 To find the list of authorised binding corporate rules by the ICO go to http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

44 Schedule 3(6)(c) to the DPA.

VI PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The ICO is responsible for enforcing the DPA. In the event of a breach the ICO may:

a issue information notices requiring organisations to provide the ICO with specified information within a certain time period;

b issue undertakings committing an organisation to a particular course of action to improve its compliance;

c issue enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law;

d conduct consensual assessments (audits) to check organisations are complying. In the past, the ICO's audit activities have been limited to assessments carried out with the consent of the organisations concerned. Now, however, the ICO may also issue an 'assessment notice', which enables it to inspect a government department or an organisation of a designated description to see whether it is complying with the data protection principles. The ICO does not need the organisation's consent to do this if it has issued the notice;

e issue assessment notices to conduct compulsory audits[45] to assess whether organisations processing personal data follow good practice (data protection only);

f issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010, or serious breaches of the PECR occurring on or after 26 May 2011;

g prosecute those who commit criminal offences under the DPA. The ICO liaises with the Crown Prosecution Service to bring criminal prosecutions against organisations and individuals for breaches of the DPA; and

h report to Parliament on data protection issues of concern.

The FCA also has enforcement powers and can impose financial penalties on financial services organisations for failure to comply with their obligations to protect customer data.

ii Recent ICO-led enforcement cases

On 20 August 2015, Google, Inc was ordered by the ICO to remove nine search results after the ICO ruled that they linked to information about a person that was no longer relevant.

On 6 August 2015, the ICO issued a £180,000 monetary penalty because of the loss by a company of computer equipment containing a significant amount of customers' details.

A recruitment company was prosecuted for failing to notify the ICO and was fined £375 and ordered to pay costs of £774.20 and a victim surcharge of £38.

45 For central government organisations.

The owner of a marketing company was prosecuted for failing to notify the ICO of changes to his notification at Willesden Magistrates Court in July 2014. He was fined £4,000, ordered to pay costs of £2,703 and a £400 victim surcharge.

A man who ran a company that tricked organisations into revealing personal details about customers was ordered to pay a total of £20,000 in fines and prosecution costs, as well as a confiscation order of over £69,000 at a hearing at Isleworth Crown Court in April 2014.

In August 2014, a £180,000 monetary penalty notice was served on the Ministry of Justice for serious failings in the way prisons in England and Wales have been handling people's information.

VII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA applies to a data controller established in the United Kingdom and processing personal data in the context of that establishment. It will also apply to foreign organisations not established in the United Kingdom, or in any other EEA state, that use equipment located in the United Kingdom (e.g., a service provider processing personal data in the United Kingdom) for processing personal data otherwise than for the purposes of transit through the United Kingdom. Data controllers not established in the United Kingdom or any other EEA country and processing personal data through equipment located in the United Kingdom must nominate a representative established in the United Kingdom and comply with the data principles and requirements under the DPA.

VIII CYBERSECURITY AND DATA BREACHES

i Cybersecurity

The Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA provides a framework for the lawful interception of communications, access to communications data, surveillance and the use of covert human intelligence sources (undercover agents), and for regulating the powers of UK public bodies to carry out surveillance and investigations.

The Secretary of State has issued codes of practice relating to the exercise and performance of the powers and duties conferred or imposed under RIPA, which provide guidance on the procedures to be followed when exercising these powers and duties. Six codes of practice are currently in force.[46]

In its employment practices code and supplementary guidance, the ICO explains that interception of employees' communications without consent is allowed under

46 Covert Human Intelligence Sources: Code of Practice, 8 September 2010; Interception of Communications: Code of Practice, 8 September 2010; Investigation of Protected Electronic Information: Code of Practice, 8 September 2010; Covert Surveillance and Property Interference: Revised Code of Practice, 8 September 2010; Acquisition and Disclosure of Communications Data: Code of Practice, 8 September 2010; and Interception of Communications: Code of Practice, 8 September 2010.

RIPA only if the interception is solely for monitoring of recording communications that: (1) involve the business entering into transactions; or (2) relate in another way to the business or take place in some other way in the course of carrying on the business. These categories cover most business communications, but they do not include personal communications by employees unless they relate to the business. In addition, interceptions are also lawful under RIPA when authorised by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Under these Regulations, interception without consent is allowed if it is part of monitoring (or recording) business communications for one of the following purposes:

a to establish the existence of facts (e.g., to collect evidence of transactions such as those involved in telephone banking or to keep records of other communications where the specific facts are important, such as being able to prove that a customer has been given certain advice);

b to ascertain that the business is complying with regulatory or self-regulatory procedures (e.g., to check that workers selling financial services are giving customers the 'health warnings' required under financial services regulation);

c to ascertain or demonstrate standards that workers are achieving (e.g., to check the quality of email responses sent by workers to customer enquiries);

d to show the standards workers ought to achieve (e.g., for staff training);

e to prevent or detect crime (e.g., to check that workers or others are not involved in defrauding the business);

f to investigate or detect unauthorised use of the telecommunications system (e.g., to ensure that workers do not breach the employer's rules on use of the system for business purposes, for example by sending confidential information by email without using encryption if this is not allowed. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised); and

g to ensure the security of the system and its effective operation (e.g., to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

The Data Retention and Investigatory Powers Act 2014

On 17 July 2014, the DRIP Act received Royal Assent, only three days after being presented to Parliament.

The DRIP Act is a direct consequence of the Court of Justice of the European Union decision of 8 April 2014, which declared the Data Retention Directive[47] invalid. This was on the basis that requiring the retention of the data and allowing competent

47 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

national authorities to access those data constitutes in itself an interference with the fundamental right to respect for private life and with the fundamental right to the protection of personal data.

Under the DRIP Act, the Secretary of State may, by notice, require a public telecommunications operator to retain relevant communications for a period that must not exceed 12 months if he or she considers that this is necessary and proportionate for one or more of the purposes for which communications may be obtained under the Regulation of Investigatory Powers Act 2000.

One year after receiving royal assent, the English High Court issued a landmark judgment declaring the DRIP Act unlawful.[48] The High Court ruled that a number of the provisions in the DRIP Act were incompatible with EU human rights law. However, the ruling was suspended until 31 March 2016 to give UK legislators time to implement appropriate safeguards.

UK cybersecurity strategy

In November 2011, the Cabinet Office published the UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, with four objectives for the UK government to achieve by 2015: (1) tackling cybercrime and making the United Kingdom one of the most secure places in the world to do business; (2) to be more resilient to cyberattacks and better able to protect our interests in cyberspace; (3) to create an open, stable and vibrant cyberspace, which the UK public can use safely and that supports open societies; and (4) to have the cross-cutting knowledge, skills and capability it needs to underpin all our cybersecurity objectives.

In March 2013, the government launched the Cyber-security Information Sharing Partnership to facilitate the sharing of intelligence and information on cybersecurity threats between the government and industry.

The UK government has also recently developed the Cyber Essentials scheme, which aims to provide clarity on good cybersecurity practice.

Along with the Cyber Essentials scheme, the government has published the Assurance Framework, which enables organisations to obtain certifications to reassure customers, investors, insurers and others that they have taken the appropriate cybersecurity precautions. The voluntary scheme is currently open and available to all types of organisation.

The government launched in June 2015 a new online cybersecurity training course to help the procurement profession stay safe online.

In July 2015, the government announced the launch of a new voucher scheme to protect small businesses from cyberattacks, which will offer micro, small and medium-sized businesses up to £5,000 for specialist advice to boost their cybersecurity and protect new business ideas and intellectual property.

48 *David & Ors v. Secretary of State for the Home Department* [2015] EWHC 2092 (Admin).

Data breaches

Under the DPA, there is no requirement to report security breaches to the ICO and the individuals involved. Although there is no legal obligation on data controllers to report security breaches, the ICO believes that serious breaches should be brought to its attention. According to the ICO, there should be a presumption to report a breach to the ICO if a significant volume of personal data is concerned and also where smaller amounts of personal data are involved but there is still a significant risk of individuals suffering substantial harm.[49] The ICO has issued varied guidance on how to manage security breaches and how to make a security-breach notification.[50]

Also, under the PECR[51] and the Notification Regulation,[52] internet and telecoms service providers must report breaches to the ICO no later than 24 hours after the detection of a personal data breach where feasible.[53] The ICO has published guidance on this specific obligation to report breaches.[54]

IX OUTLOOK

The ICO is planning to introduce a consumer-facing privacy-seal scheme operated by the UK Accreditation Service. These schemes will act as a 'stamp of approval' and organisations will be able to display the seal on their products as a means to highlight the organisation's commitment to maintaining privacy standards. In an update issued in August 2015, the ICO stated that it intends to introduce the scheme before the proposed EU Data Protection Regulation comes into force.

Negotiations for the proposed EU Data Protection Regulation are approaching the final stages, with adoption expected by the end of 2015 or early 2016. In light of this, the ICO is encouraging UK businesses to consider now the impact of the proposed Regulation, and has highlighted a number of key areas of focus, including accountability, consent, data breach management and 'privacy by design'. These are all fundamental concepts under the proposed Regulation.

49 ICO, Guidance on Notification of Data Security Breaches to the Information Commissioner's Office, 27 July 2012.

50 ICO, Guidance on Data Security Breach Management, 12 December 2012, and Guidance on Notification of Data Security Breaches to the Information Commissioner's Office, 27 July 2012, and the previous version published on 27 March 2008.

51 PECR Regulation 5A(2).

52 Commission Regulation No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (the Notification Regulation), which entered into force on 25 August 2013.

53 Article 2 of the Notification Regulation. The content of the notification is detailed in Annex 1 to the Notification Regulation.

54 ICO, Guidance on Notification of PECR Security Breaches, 26 September 2013.

Chapter 27

UNITED STATES

Alan Charles Raul, Tasha D Manoranjan and Vivek K Mohan[1]

I OVERVIEW

Although not universally acknowledged, the US commercial privacy regime is arguably the oldest, most robust, well developed and effective in the world. The US privacy system has a relatively flexible and non-prescriptive nature, relying more on *post hoc* government enforcement and private litigation, and on the corresponding deterrent value of such enforcement and litigation, than on detailed prohibitions and rules. With certain notable exceptions, the US system does not apply a 'precautionary principle' to protect privacy, but rather allows injured parties (and government agencies) to bring legal action to recover damages for, or enjoin a party from, 'unfair or deceptive' business practices. However, US federal law does impose affirmative prohibitions and restrictions in certain commercial sectors, such as those involving financial and medical data, and electronic communications, as well as with respect to children's privacy, background investigations and 'consumer reports' for credit or employment purposes, and certain other specific areas. State laws add numerous additional privacy requirements.

Legal protection of privacy in civil society has been recognised in the US common law since 1890 when the article 'The Right to Privacy' was published in the *Harvard Law Review* by Professors Samuel D Warren and Louis D Brandeis. Moreover, from its conception by Warren and Brandeis, the US system for protecting privacy in the commercial realm has been focused on addressing technological innovation. The Harvard

1 Alan Charles Raul is a partner and Tasha D Manoranjan and Vivek K Mohan are associates at Sidley Austin LLP. Passages of this chapter were originally published in 'Privacy and data protection in the United States', *The debate on privacy and security over the network: Regulation and markets, 2012*, Fundación Telefónica; and Raul and Mohan, 'The Strength of the U.S. Commercial Privacy Regime', 31 March 2014, a memorandum to the Big Data Study Group, US Office of Science and Technology Policy.

professors astutely noted that '[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […] the right "to be let alone"'. In 1974, Congress enacted the federal Privacy Act, regulating government databases, and found that 'the right to privacy is a personal and fundamental right protected by the Constitution of the United States'. It is generally acknowledged that the US Privacy Act represented the first official embodiment of the fair information principles and practices that have been incorporated in many other data protection regimes, including the European Union's 1995 Data Protection Directive.

The United States has also led the way for the world not only on establishing model legal data protection standards in the 1974 Privacy Act, but also in terms of imposing affirmative data breach notification and information security requirements on private entities that collect or process personal data from consumers, employees and other individuals. The state of California was the path-breaker on data security and data breach notification by first requiring in 2003 that companies notify individuals whose personal information was compromised or improperly acquired. Since then, approximately 47 states, the District of Columbia and other US jurisdictions, and the federal banking, healthcare and communications agencies have also required companies to provide mandatory data breach notification to affected individuals, and imposed affirmative administrative, technical and physical safeguards to protect the security of sensitive personal information. Dozens of other medical and financial privacy laws also exist in various states. There is, however, no single omnibus federal privacy law in the United States. Moreover, there is no designated central data protection authority in the United States, though the Federal Trade Commission (FTC) has primarily assumed that role for consumer privacy. The FTC is independent of the President, and is not obliged (though it is encouraged) to respect the Administration's perspective on the proper balance between costs and benefits with respect to protecting data privacy. The Chairperson of the FTC is designated by the President, however, and may be removed as Chair (though not as one of the FTC's five Commissioners) at the discretion of the President.

As in the EU and elsewhere, privacy and data protection are balanced in the United States in accordance with other rights and interests that societies need to prosper and flourish, namely economic growth and efficiency, technological innovation, property and free speech rights and, of course, the values of promoting human dignity and personal autonomy. The most significant factor in counterbalancing privacy protections in the United States, perhaps, is the right to freedom of expression guaranteed by the First Amendment. Preserving free speech rights for everyone certainly entails complications for a 'right to be forgotten' since one person's desire for oblivion may run counter to another's sense of nostalgia (or some other desire to memorialise the past for good or ill).

The First Amendment has also been interpreted to protect the people's right to know information of public concern or interest, even if it trenches to some extent on individual privacy. Companies have also been deemed to have a First Amendment right to communicate relatively freely with their customers by exchanging information in both directions (subject to the information being truthful, not misleading and otherwise not the subject of an unfair or deceptive business practice).

The dynamic and robust system of privacy governance in the United States marshals the combined focus and enforcement muscle of the US Federal Trade Commission, state attorneys general, the Federal Communications Commission, the

Securities and Exchange Commission, the Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services, the Department of Education, the judicial system, and last – but certainly not least – the highly motivated and aggressive US private plaintiffs' bar. Taken together, this enforcement ecosystem has proven to be nimble, flexible and effective in adapting to rapidly changing technological developments and practices, responding to evolving consumer and citizen expectations, and serving as a meaningful agent of deterrence and accountability. Indeed, the US enforcement and litigation-based approach appears to be particularly well suited to deal with 'recent inventions and business methods' – namely new technologies and modes of commerce – that pose ever changing opportunities and unpredictable privacy challenges.

II THE YEAR IN REVIEW

Privacy and cybersecurity remain hot topics for regulators, and the past year has seen a number of agencies that previously exercised a limited mandate in this area issue guidance and pursue enforcement actions. The courts have also been active, and a number of recent cases promise to reshape the legal landscape for years to come. Nonetheless, it is difficult to foresee the full legal impact of major cybersecurity incidents, ranging from a breach at the federal Office of Personnel Management to the wholesale compromise of the emails and records belonging to Sony Pictures Entertainment, and the penetration of user accounts of the dating website Ashley Madison. While Congress has been stymied in adopting 'information sharing' legislation, in February 2015, President Obama signed an Executive Order that encourages and establishes information sharing and analysis organisations, or ISAOs, to share cyberthreat information between the government and private sector.

The FTC scored a major victory with regard to the scope of cybersecurity authority in federal court. The Third Circuit Court of Appeals affirmed the Commission's authority to regulate data security in a much-anticipated ruling, *Federal Trade Commission v. Wyndham Worldwide Corp*, No. 14-3514 (3rd Cir. 24 August 2015). The Third Circuit held that the FTC has the authority to bring data security actions based on the general mandate of Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. In other words, the FTC's assertion of jurisdiction to enforce data security standards under broad, general language has been upheld against a challenge claiming that the agency did not have authority in the absence of an express grant of privacy or cybersecurity power by Congress. As detailed below, the FTC has continued to play a leading role at the federal level on these issues.

Other government agencies announced their focus on these issues, often issuing guidance for entities that fall within their regulatory sphere of influence. The Securities and Exchange Commission (SEC) has issued guidance on information security and data breach preparedness. The Department of Justice has also issued guidance for addressing data breach incidents, and for interacting with federal law enforcement.

Very significantly the FCC has reclassified broadband internet access services as subject to 'common carrier' regulation by that agency in a new Open Internet Order concerning 'network neutrality'. Under the Order, the FCC indicated it intends to issue

a substantial forthcoming rulemaking regarding privacy obligations for internet access providers pursuant to customer proprietary network information (CPNI) provisions in the Communications Act. Even before this new rule has been issued, the FCC has been increasingly active in enforcement, including through the imposition of a $25 million penalty against a major telecommunications provider in connection with a data breach affecting consumer phone records. Smaller carriers have also been subjected to significant penalties for alleged privacy and data security violations.

On 1 June 2015, Section 215 of the Patriot Act expired. This provision was used to justify the controversial National Security Agency (NSA) programme collecting bulk phone metadata. While the programme was fully disclosed in 2006 in the media, leaks of NSA documents by former NSA contractor Edward Snowden caused an international furore. Congress subsequently reauthorised the lapsed provision, but in a modified form limiting the NSA to engage in automatic bulk collection of metadata. Broader efforts at surveillance reform have little momentum.

States have continued to push privacy and cybersecurity initiatives forward. Connecticut, Nevada, North Dakota and Washington have all updated their breach notification laws. Connecticut has become the first state to impose a requirement to provide affected data subjects free credit-reporting services for at least one year. State legislation related to social media privacy also continues to be popular. Connecticut became the twenty-first state to enact a measure prohibiting employers from forcing employees or job applicants to 'friend' them or otherwise share the details of their personal online accounts; and Oregon passed a law prohibiting employers from requiring personal social media accounts as a condition of employment. Other significant state initiatives include New Jersey's enactment of a version of a long-stalled federal bill to protect car 'black box' data, Florida's ban on the use of drones to photograph individuals on private property, and Virginia's new state level ISAO to share cyberthreat information among state entities as well as between private sector entities.

In data breach litigation, two recent settlements highlight the struggle of determining who is responsible for costs related to corporate data breaches. The major retailer Target agreed to pay $19 million as reimbursement for MasterCard's losses from claims relating to Target's December 2013 data breach. But just a few weeks later, the deal fell apart as the parties failed to get consent from at least 90 per cent of MasterCard issuing banks and credit unions claiming their losses amount to over $160 million. In August, Target and Visa agreed on a settlement of $67 million. Separately, a settlement of $10 million in a class-action suit received preliminary approval by the courts in March. And amid this uncertainty, large-scale breaches continue, with an announcement coming from the IRS of the theft of over 100,000 taxpayers' data, and then another massive breach announced by the Office of Personnel Management potentially affecting over 21 million current and former federal employees.

i FTC actions

The Third Circuit's decision in *Wyndham*, upholding the FTC's data security authority, is probably the most important consumer protection-related development for the Commission over the past year. The FTC has remained active on these issues, both in issuing guidance as well as in bringing enforcement actions.

On 20 May, the FTC Business Blog featured a post on what companies should expect 'if the FTC comes to call'. The use of the blog for what was an interesting policy development may itself merit mention. The posting itself was particularly significant because it indicated for the first time that the FTC will view a company more 'favourably' if it has reported the breach to and cooperated with law enforcement. This aligns with recent DOJ guidance that recommended early cooperation with law enforcement and even establishing a law-enforcement point of contact for breach preparedness.

The blog posting also advised companies that the FTC typically begins a data security investigation informally by reviewing publicly available information or reaching out to the company directly. If the agency concludes that a full investigation is necessary, it will send the company formal requests for documents, information, interviews or testimony, and may interview third parties, including vendors, about the company's data security practices. The FTC will then determine whether the company's general data security practices are reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, the cost of available security safeguards, and whether the company complies with any applicable data security laws, like the Gramm-Leach-Bliley Act. If the investigation relates to a breach, the FTC will also seek information about the circumstances surrounding the breach, the company's response and how the breach affected consumers' personal information. Finally, the FTC's blog post concluded by assuring the public that it closes more cases than it brings, often finding that a company's data security practices were reasonable. It made no mention of the cost for companies to respond to these often expensive 'informal' investigations.

The FTC settled charges with Snapchat in May 2014 over the company's alleged deceptive privacy and confidentiality marketing promises. According to the complaint, the company, which currently transmits over 700 million messages back and forth each day, marketed its messaging services by telling users that the messages 'disappear forever', while in reality, the messages can be saved in several ways. In addition, the FTC alleged that Snapchat transmitted users' location data and transmitted sensitive information like address book contacts, although the company told consumers it did not collect such information. The settlement prohibits Snapchat from misrepresenting how it maintains the privacy and confidentiality of user information and the company will also have to start a privacy programme that will be independently monitored for 20 years. If the company does not comply, it could face fines. The company has said it has resolved most of these concerns over the past year and has improved the wording of its privacy policy, app description and in-app just-in-time notifications.

The Court of Justice of the European Union (CJEU) has had an outsize impact on privacy and data protection issues that impact US companies. The US fallout from the 'right to be forgotten' ruling and the decision that held the US-EU Safe Harbor to be invalid remain to be seen, but the FTC's involvement in both issues is notable.

Speaking at a US Council for International Business event, FTC Commissioner Julie Brill pointed to last year's decision by the CJEU regarding the right to be forgotten as something that could inform a 'right to obscurity' in the United States. The EU decision required search engines to delete links harmful to an individual's privacy interest when there is no other compelling public service. The broad EU implementation would face certain First Amendment challenges in the United States, but as Commissioner Brill pointed out, certain aspects of such a right are already US law. As an example, she

pointed to the Fair Credit Reporting Act, which prohibits certain information from being used to inform credit reports after a certain period, and that US law also allows expungement of criminal records in some circumstances. Commissioner Brill indicated that the right to obscurity could be well applied to information held by data brokers. The implementation of the right to obscurity in that case could require brokers to allow individuals to see information in their files and either correct or expunge it.

The CJEU opinion on the US-EU Safe Harbor comes despite significant efforts by EU and US officials to negotiate on a set of agreed changes to the agreement; the final points of negotiation were on national security issues, which ultimately formed the crux of the CJEU decision. Importantly, the CJEU decision comes despite significant steps towards cooperation across the Atlantic; on 9 March, the FTC and the Dutch Data Protection Agency signed a memorandum of understanding to enhance cooperation on privacy-related matters. The agreement, which is similar to ones signed by the FTC with Ireland in 2013 and the United Kingdom in 2014, is part of the agency's push to work more closely with foreign authorities in investigating and enforcing privacy violations. While not legally binding, it allows both countries to use information they receive to investigate, prosecute or prevent criminal privacy violations, including those predating the agreement. The agreement also outlines specific procedures to keep the information private, such as encrypting transmitted information and redacting personally identifiable information if the data is made publicly available. Under the agreement, shared information can only be further disclosed to third parties with the other party's permission or knowledge.

The FTC has a dual mandate – consumer protection and competition, and privacy issues have permeated across the internal walls. The Director of the FTC Bureau of Competition, Deborah L Feinstein, has indicated that privacy is growing as a part of the Commission's merger reviews, as the issue is becoming more important to consumers. Privacy could be considered as a form of actionable non-price competition. Although the FTC has yet to challenge a transaction because it would impede competition in privacy technology, such an action would not be entirely without precedent. The Commission recognised in 2007 that mergers may adversely affect consumer privacy. Additionally, the European Commission examined the issue in considering a merger between TomTom and TeleAtlas in 2008. This increased focus on privacy competition may incentivise companies to undertake due diligence of both their own and target acquisitions' privacy practices and policies, and consider how privacy protections may be strengthened as part of the merger process.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The United States has specific privacy laws for the types of citizen and consumer data that are most sensitive and at risk: financial, insurance and medical information; information about children and students; telephone, internet and other electronic communications and records; credit and consumer reports and background investigations, at the federal level, and a further extensive array of specific privacy laws at the state level. Moreover, the United States is the unquestioned world leader in mandating information security

and data breach notification, without which information privacy is not possible. If one of the sector-specific federal or state laws does not cover a particular category of data or information practice, then the Federal Trade Commission Act, and each state's 'little FTC Act' analogue, comes in to play. Those general consumer protection statutes broadly, flexibly and comprehensively proscribe (and authorise tough enforcement against) unfair or deceptive acts or practices. The FTC is the *de facto* privacy regulator in the United States. It should also be noted that state attorneys general, and private plaintiffs, can also enforce privacy standards under analogous 'unfair and deceptive acts and practices' standards in state law. Additionally, information privacy is further protected by a network of common law torts, including invasion of privacy, public disclosure of private facts, 'false light', appropriation or infringement of the right of publicity or personal likeness, and of course, remedies against general misappropriation or negligence. In short, there are no substantial lacunae in the regulation of commercial data privacy in the United States. In taking both a general (unfair or deceptive) and sectoral approach to commercial privacy governance, the United States has empowered government agencies to oversee data privacy where the categories and uses of data could injure individuals.

The FTC Act

Section 5 of the Federal Trade Commission Act (the FTC Act) prohibits 'unfair or deceptive acts or practices in or affecting commerce'. While the FTC Act does not expressly address privacy or information security, the FTC applies Section 5 to information privacy, data security, online advertising, behavioural tracking and other data-intensive, commercial activities. The FTC has brought successful enforcement actions under Section 5 against companies that failed to adequately disclose their data collection practices, failed to abide by the promises made in their privacy policies, failed to comply with their security commitments or failed to provide a 'fair' level of security for consumer information.

Under Section 5, an act or practice is deceptive if: (1) there is a representation or omission of information likely to mislead a consumer acting reasonably under the circumstances; and (2) the representation or omission is 'material' – defined as an act or practice 'likely to affect the consumer's conduct or decision with regard to a product or service'. An act or practice is 'unfair' under Section 5 if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and lacks countervailing benefits to consumers or competition.

The FTC takes the position that companies must disclose their privacy practices adequately, and that in certain circumstances, this may require particularly timely, clear and prominent notice, especially for novel, unexpected or sensitive uses. The FTC brought an enforcement action in 2009 against Sears for allegedly failing to adequately disclose the extent to which it collected personal information by tracking the online browsing of consumers who downloaded certain software. The consumer information allegedly collected included 'nearly all of the Internet behavior that occurs on […] computers'. The FTC required Sears to prominently disclose any data practices that would have significant unexpected implications in a separate screen outside any user agreement, privacy policy or terms of use.

Section 5 is also generally understood to prohibit a company from using previously collected personal data in ways that are materially different, and less protective, than what it initially disclosed to the data subject, without first obtaining the individual's additional consent.

The FTC staff has also issued extensive guidance on online behavioural advertising, emphasising four principles to protect consumer privacy interests: (1) transparency and control, giving meaningful disclosure to consumers, and offering consumers choice about information collection; (2) maintaining data security, and limiting data retention; (3) express consent before using information in a manner that is materially different from the privacy policy in place when the data was collected; and (4) express consent before using sensitive data for behavioural advertising. The FTC's report does not, however, require opt-in consent for the use of non-sensitive information in behavioural advertising.

Fair information practice principles

The innovative American privacy doctrine elaborated theories for tort and injunctive remedies for invasions of privacy (including compensation for mental suffering). The Warren–Brandeis right to privacy, along with the right to be let alone, was followed in 1973 by the first affirmative government undertaking to protect privacy in the computer age. The new philosophy was expressed in The Secretary's Advisory Committee on Automated Personal Data Systems, published by the US Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services). This report developed the principles for 'fair information practices' that were subsequently adopted by the United States in the 1974 Privacy Act, and ultimately, by the European Union in 1995 in its Data Protection Directive. The fair information practice principles established in the United States in 1973–1974 remain largely operative around the world today in regimes and societies that respect information privacy rights of individuals. The fundamental US HEW/Privacy Act principles were:

a there must be no personal data record-keeping systems whose very existence is secret;

b there must be a way for an individual to find out what information about him or her is in a record and how it is used;

c there must be a way for an individual to prevent information about him or her obtained for one purpose from being used or made available for other purposes without his or her consent;

d there must be a way for an individual to correct or amend a record of identifiable information about him or her; and

e any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Classification of data

The definitions of personal data and sensitive personal data vary by regulation. The FTC considers information that can reasonably be used to contact or distinguish an individual (including IP addresses) to constitute personal data (at least in the context of

children's privacy). Generally, sensitive data includes personal health data, credit reports, personal information collected online from children under 13, precise location data, and information that can be used for identity theft or fraud.

Federal laws

Congress has passed laws protecting personal information in the most sensitive areas of consumer life, including health and financial information, information about children, and credit information. Various federal agencies are tasked with rule making, oversight, and enforcement of these legislative directives.

The scope of these laws and the agencies that are tasked with enforcing them is formidable. Laws such as Children's Online Privacy Protection Act of 1998, the Health Insurance Portability and Accountability Act of 1996, the Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act or GLBA), the Fair Credit Reporting Act, the Electronic Communications Privacy Act, the Communications Act (regarding CPNI) and the Telephone Consumer Protection Act of 1991, to name just a few, prescribe specific statutory standards to protect the most sensitive consumer data.

State laws

In addition to the concurrent authority that state attorneys general share for enforcement of certain federal privacy laws, state legislatures have been especially active on privacy issues that states view worthy of targeted legislation. In the areas of online privacy and data security alone, state legislatures have passed laws covering a broad array of privacy-related issues,[2] cyberstalking,[3] data disposal,[4] privacy policies, security breach notification,[5] employer access to employee social media accounts,[6] unsolicited commercial communications[7] and electronic solicitation of children,[8] to name but a few.

California is viewed as a leading legislator in the privacy arena, and its large population and high-tech sector means that the requirements of California law receive particular attention and often have *de facto* application to businesses operating across the

2 See www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

3 See www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx.

4 See www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

5 See www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

6 See www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

7 See www.ncsl.org/research/telecommunications-and-information-technology/unsolicited-commercial-communication-laws.aspx.

8 See www.ncsl.org/research/telecommunications-and-information-technology/electronic-solicitation-or-luring-of-children-sta.aspx.

United States.[9] The combined legislative and enforcement authority of federal and state governments ensures that the policy leadership articulated at the federal level – like the White House's 2012 Privacy Report – can be implemented effectively in practice.

Co-regulation and industry self-regulation

To address concerns about privacy practices in various industries, industry stakeholders have worked with government, academics, and privacy advocates to build a number of co-regulatory initiatives that adopt domain-specific, robust privacy protections that are enforceable by the FTC under Section 5 and by state attorneys general pursuant to their concurrent authority. These cooperatively-developed accountability programmes establish expected practices for use of consumer data within their sectors, which is then subject to enforcement by both governmental and non-governmental authorities. This approach has had notable success, such as the development of the 'About Advertising' icon by the Digital Advertising Alliance and the opt-out for cookies set forth by the Network Advertising Initiative.[10] Companies that assert their compliance with, or membership in, these self-regulatory initiatives must comply with these voluntary standards or risk being deemed to have engaged in a deceptive practice. The same is true for companies that publish privacy policies – a company's failure to comply with its own privacy policy is a quintessentially deceptive practice. It should also be noted that various laws require publication or provision of privacy policies, including for example, the GLBA (financial data), HIPAA (health data) and California law (websites collecting personal information). In addition, voluntary membership or certification in various self-regulatory initiatives also requires posting of privacy policies, which then become enforceable by the FTC, state attorneys general and private plaintiffs claiming detrimental reliance on such policies.

ii General obligations for data handlers

There is no general requirement to register databases in the United States. Depending on the context, data handlers may be required to provide data subjects with pre-collection notice, and the opportunity to opt out for use and disclosure of regulated personal information. Information that is considered sensitive personal information, such as health information, may involve opt-in rules. The FTC considers it a deceptive trade practice if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was obtained.

iii Technological innovation and privacy law

Electronic marketing is extensively regulated in the United States through a myriad of laws. The CAN-SPAM Act is a federal law governing commercial email messages. Generally, a company is permitted to send commercial emails to anyone under CAN-SPAM, provided these conditions are met: the recipient has not opted out of

9 See https://oag.ca.gov/privacy/privacy-laws.

10 See www.aboutads.info/; www.networkadvertising.org/choices/?partnerId=1//.

receiving such emails from the company, the email identifies the sender and the sender's contact information, and the email has instructions on how to easily and at no cost opt out of future commercial emails from the company.

Generally, express, written consent is required for companies to send marketing text messages. Marketing texts are a significant class action risk area.

There is no specific federal law that regulates the use of cookies and other similar online tracking tools. However, the use of tracking mechanisms should be carefully and fully disclosed in a company's website privacy policy. Additionally, it is a best practice for websites that allow online behavioural advertising to participate in the Digital Advertising Alliance code of conduct, which enables users to easily opt out of being tracked for these purposes. California law imposes further requirements on online tracking. California requires companies that track personally identifiable information over time and multiple websites to disclose how the company responds to 'do-not-track' signals and whether users can opt out of such tracking.

Location tracking is currently a subject of interest and debate. Federal Communications Commission regulations govern the collection and disclosure of certain location tracking by the telecommunications providers (generally speaking, telephone carriers). Additionally, the FTC and California have issued best-practice recommendations for mobile apps and mobile app platforms.

iv Specific regulatory areas

The US system of privacy is composed of laws and regulations that focus on particular industries (financial services, health care, communications), particular activities (i.e., collecting information about children online) and particular types of data.

Federal

Financial privacy

For financial privacy, the federal banking agencies and the FTC were, until recently, primarily responsible for enforcing consumer privacy under the GLBA, which applies to financial institutions. Following the recent Dodd-Frank legislation, such laws will be primarily (but not exclusively) enforced by the new Consumer Financial Protection Bureau, which has significant, independent regulatory and enforcement powers. The FTC, however, will remain primarily responsible for administering the Fair Credit Reporting Act, along with the general unfair and deceptive acts and practices standards under the FTC Act and the Children's Online Privacy Protection Act 1998 (COPPA), which imposes affirmative privacy and security duties on entities that collect personal information from children under 13 years of age.

The Financial Services Modernization Act of 1999 or GLBA addresses financial data privacy and security by establishing standards for safeguarding customers' 'non-public personal information' – or personally identifiable financial information – stored by 'financial institutions', and by requiring financial institutions to provide notice of their information-sharing practices. In brief, the GLBA requires financial institutions: to provide notices of policies and practices regarding disclosure of personal information;

to prohibit the disclosure of such data to unaffiliated third parties unless consumers are provided the right to opt out of such disclosure or other exceptions apply; and to establish safeguards to protect the security of personal information.

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003, imposes requirements on entities that possess or maintain consumer credit reporting information, or information generated from consumer credit reports. Consumer reports are 'any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility' for credit, insurance, employment, or other similar purposes. The FCRA mandates accurate and relevant data collection to give consumers the ability to access and correct their credit information, and limits the use of consumer reports to permissible purposes, such as employment and extension of credit or insurance.[11]

Healthcare privacy

For healthcare privacy, agencies within the Department of Health and Human Services administers and enforces the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). HIPAA was enacted to create national standards for electronic healthcare transactions, and the US Department of Health and Human Services has promulgated regulations to protect privacy and security of personal health information (PHI). Patients generally have to opt in before their information can be shared with other organisations.[12] HIPAA applies to 'covered entities', which include health plans, healthcare clearing houses, and healthcare providers that engage in electronic transactions as well as, via HITECH, service providers to covered entities that need access to PHI to perform their services. It also imposes requirements in connection with employee medical insurance.

'Protected health information' is defined broadly as 'individually identifiable health information […] transmitted or maintained in electronic media' or in 'any other form or medium'. 'Individually identifiable health information' is defined as information that is a subset of health information including demographic information that 'is created or received by a health care provider, health plan, employer, or health care clearinghouse'; and 'relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual' and either identifies the individual or provides a reasonable means by which to identify the individual. HIPAA also does not apply to 'de-identified' data.

11 Available at www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act.

12 Available at www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf.

A 'business associate' is an entity that performs or assists a covered entity in the performance of a function or activity that involves the use or disclosure of PHI (including, but not limited to, claims processing or administration activities). Business associates are required to enter into agreements, called business associate agreements, requiring business associates to use and disclose PHI only as permitted or required by the business associate agreement or as required by law, and to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the business associate agreement, as well as numerous other provisions regarding confidentiality, integrity and availability of electronic PHI. HIPAA and HITECH not only restrict access to and use of medical information, but also impose stringent information security standards.

Communications privacy

For communications privacy, the Federal Communications Commission (FCC), the Department of Justice and, to a considerable extent, private plaintiffs can enforce the data protection standards in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act and various sections of the Communications Act, which include specific protection for CPNI such as telephone call records. The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communication and related records. The Computer Fraud and Abuse Act prohibits hacking and other forms of harmful and unauthorised access or trespass to computer systems, and can often be invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks. The FCC, however, is the primary regulator for communications privacy issues, and has been active over the past year.

The FCC shares jurisdiction with the FTC on certain privacy and data security issues, including notably on the issue of robocalls as governed by the Telephone Consumer Protection Act. There has been significant regulatory activity in the past year, including guidance released by the FCC on auto-dialers in August 2015, not to mention substantial private litigation driven by the statutory penalties provided for by TCPA. The FCC stated in June that complaints regarding unwanted calls are the largest category of complaints received by the FCC – numbering over 215,000 complaints in 2014 alone.[13]

The FCC entered the realm of data security regulation last October when the FCC announced a proposed fine of $10 million, claiming that a telecommunications service provider failed to protect customers' sensitive personal information (the case later settled for $3.5 million). A few days later, the FCC also announced that it joined the Global Privacy Enforcement Network, a group of international privacy regulators and enforcers of which the FTC is also a member.

On 26 February 2015, the FCC adopted the Open Internet Order to reclassify broadband internet access service as a telecommunications service under Title II of the Communications Act of 1934. In doing so, the FCC found that applying the privacy requirements of the Communications Act (Section 222) to broadband internet

13 Available at https://www.fcc.gov/document/fcc-strengthens-consumer-protections-against-unwanted-calls-and-texts.

access services is in the public interest and necessary for the protection of customers. Section 222 imposes a duty on telecommunications carriers to protect the confidentiality of proprietary information obtained from their customers or other carriers, and imposes special rules for use and disclosure of information related to customers' phone service and usage, known as CPNI. The FCC stated that its Open Internet rules are 'designed to protect free expression and innovation on the Internet and promote investment in the nation's broadband networks'.[14] Among other things, the rules prohibit paid prioritisation, in which broadband providers could otherwise use 'fast lanes' to favour higher-paying internet traffic over other lawful traffic. The Open Internet rules took effect on 12 June 2015. The FCC Order is also significant because, despite the FTC's expansive view of the reach of its jurisdiction, the FCC's Order potentially divests the FTC of jurisdiction to regulate broadband internet access services under Section 5 of the Federal Trade Commission Act and to enforce the Children's Online Privacy and Protection Act (COPPA) against broadband providers. Thus, should this Order stand, the FCC may become the primary federal regulator of privacy and information security for broadband providers. The FCC has indicated that it will issue rules in the future delineating specific privacy requirements applying Section 222's privacy requirements to broadband internet access services. In the meantime, on 20 May 2015, the agency's Enforcement Bureau provided the following guidance regarding the Open Internet Privacy Standard, and indicated that ISPs should take reasonable steps to protect privacy:

> *The Commission's Open Internet Order applies the core customer privacy protections of Section 222 of the Communications Act to providers of broadband internet access service (BIAS). The Commission has found that in the absence of privacy protections, a broadband provider's use of personal and proprietary information could be at odds with its customers' interests and that if consumers have concerns about the protection of their privacy, their demand for broadband may decrease. At the same time, the Commission declined to apply its existing telephone-centric rules implementing Section 222 and indicated that in the future it may adopt implementing rules that are tailored to broadband providers. As a result, the statutory provisions of Section 222 themselves will apply to broadband providers when the Open Internet Order goes into effect.*
>
> *[…]*
>
> *During this period [prior to the issuance of specific rules], the Enforcement Bureau intends to focus on whether broadband providers are taking reasonable, good-faith steps to comply with Section 222, rather than focusing on technical details. By examining whether a broadband provider's acts or practices are reasonable and whether such a provider is acting in good faith to comply with Section 222, the Enforcement Bureau intends that broadband providers should employ effective privacy protections in line with their privacy policies and core tenets of basic privacy protections.*[15]

14 Available at https://www.fcc.gov/openinternet.

15 Available at www.fcc.gov/document/isps-should-take-reasonable-steps-protect-privacy.

Children's privacy

COPPA applies to operators of commercial websites and online services that are directed to children under the age of 13, as well as general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires that these website operators post a privacy policy, provide notice about collection to parents, and obtain verifiable parental consent before collecting personal information from children, and other actions.[16]

Other federal privacy laws

Even the array of privacy laws described above is hardly comprehensive. A number of other federal privacy laws protect personal information in the areas of cable television, education, telecommunications customer information, drivers' and motor vehicle records, and video rentals. Federal laws also protect marketing activities such as telemarketing, junk faxes and unsolicited commercial email.

State legislation

In the areas of online privacy and data security alone, state legislatures have passed a number of laws covering access to employee and student social media passwords, children's online privacy, e-Reader privacy, online privacy policies, false and misleading statements in website privacy policies, privacy of personal information held by ISPs, notice of monitoring of employee email communications and internet access, phishing, spyware, security breaches, spam, and event data recorders. California is viewed as the leading legislator in the privacy arena, with many other states following its privacy laws. State attorneys general also have concurrent authority with the FTC or other federal regulators under various federal laws, such as COPPA, HIPAA and others.

The National Council of State Legislatures summarises the following state provisions regarding online privacy:

> ***Privacy Policies for Websites or Online Services***
>
> *California's Online Privacy Protection Act requires an operator […] to post a conspicuous privacy policy on its Web site or online service […] and to comply with that policy. The law, among other things, requires that the privacy policy identify the categories of personally identifiable information that the operator collects about individual consumers who use or visit its Web site [and] how the operator responds to a web browser 'Do Not Track' signal. Connecticut [r]equires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy must be 'publicly displayed' by posting on a web page and the policy must […] protect the confidentiality of Social Security numbers.*
>
> ***Privacy of Personal Information Held by Internet Service Providers***
>
> *Two states, Nevada and Minnesota, require Internet Service Providers to keep private certain information concerning their customers, unless the customer gives permission to disclose the*

16 Available at www.law.cornell.edu/USCode/text/15/6501.

information. Both states prohibit disclosure of personally identifying information, but Minnesota also requires ISPs to get permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.

False and Misleading Statements in Website Privacy Policies
Nebraska prohibits knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public. Pennsylvania includes false and misleading statements in privacy policies published on Web sites or otherwise distributed in its deceptive or fraudulent business practices statute.

Notice of Monitoring of Employee E-mail Communications and Internet Access
Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access.[17]

Children's online privacy

California prohibits websites directed to minors from advertising products based on information specific to that minor. The law also requires the website operator to permit a minor to request removal of content or information posted on the operator's site or service by the minor, with certain exceptions.[18]

IV INTERNATIONAL DATA TRANSFER

There are no significant or generally applicable data transfer restrictions in the United States; however, the United States has taken steps to provide compliance mechanisms for companies that are subject to data transfer restrictions set forth by other countries The recent ruling by the CJEU that the US-EU Safe Harbor Framework is 'invalid' has brought a considerable degree of uncertainty to the thousands of companies that rely on it as a bedrock of day-to-day global operations. Whether or not corrective measures – interim or permanent – are quickly put into place, this development is certain to have a significant impact on the businesses that rely on Safe Harbor to legitimise transfers of personal data from the EU to the United States.

While Safe Harbor was criticised and held 'invalid' by the CJEU, it has been an important tool to enhance international interoperability and cooperation. The US-EU Safe Harbor Framework has permitted the FTC to complement the EU's effort to protect European consumers' privacy. The FTC has stated that Safe Harbor is a top

17 National Conference of State Legislatures, www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

18 Calif. Bus. & Prof. Code Sections 22580–22582.

enforcement priority.[19] The FTC has brought dozens of Safe Harbor cases,[20] and the agency is committed to review on a priority basis all referrals from EU Member State authorities. On 7 April 2015, the FTC's Chairwoman, Edith Ramirez, emphasised the agency's commitment to enforcing Safe Harbor in announcing the filing and settling of two new actions against companies for (allegedly) falsely claiming that they complied with the applicable international data transfer requirements. She stated:

> *We remain strongly committed to enforcing the US-EU and US-Swiss Safe Harbor Frameworks. […] These cases send an important message that businesses must not deceive consumers about whether they hold these certifications, and by extension, the ways in which they protect consumers.*[21]

The FTC signed a memorandum of understanding[22] with Ireland's Office of the Data Protection Commissioner in June 2013 to promote communication and cooperation between the two agencies in an era when consumer information is increasingly moving across borders. The FTC also signed a memorandum of understanding with the UK Information Commissioner's Office in March 2014.[23] The memorandum of understanding is designed to promote increased cooperation and communication in both agencies' efforts to protect consumer privacy.

In 2012, the United States was approved as the first formal participant in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, and the FTC became the system's first privacy enforcement authority. The FTC's Office of International Affairs[24] works with consumer protection agencies globally to promote cooperation, combat cross-border fraud and develop best practices.[25] In particular, the FTC works extensively with the Global Privacy Enforcement Network and APEC.[26]

---

19 Available at www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-USeu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf.

20 See FTC Enforcement: Cases and Proceedings, available at www.ftc.gov/enforcement/cases-proceedings.

21 Available at https://www.ftc.gov/news-events/press-releases/2015/04/ftc-settles-two-companies-falsely-claiming-comply-international.

22 Press release, 'FTC Signs Memorandum of Understanding with Irish Privacy Enforcement Agency' (27 June 2013), available at www.ftc.gov/news-events/press-releases/2013/06/ftc-signs-memorandum-understanding-irish-privacy-enforcement.

23 www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/140306ftc-uk-mou.pdf.

24 See FTC, Office of International Affairs, www.ftc.gov/about-ftc/bureaus-offices/office-international-affairs.

25 See FTC, International Consumer Protection, www.ftc.gov/policy/international/international-consumer-protection.

26 See 'APEC Overview', Chapter 2.

V COMPANY POLICIES AND PRACTICES

A recent study of corporate privacy management[27] reveals the success of enforcement in pushing corporate privacy managers to look beyond the letter of the law to develop state-of-the-art privacy practices that anticipate FTC enforcement actions, best practices, and other forms of FTC policy guidance. Many corporate privacy managers explain that the constant threat and unpredictability of future enforcement by the FTC and parallel state consumer protection officials, combined with the deterrent effect of enforcement actions against peer companies, motivate their companies to proactively develop privacy policies and practices that exceed industry standards. Other companies respond by hiring a privacy officer or creating or expanding a privacy leadership function. The risk of enforcement also prompted companies to engage in ongoing dialogues with the FTC and state regulators.

Corporate privacy managers also emphasised that while compliance-oriented laws in other jurisdictions do not always keep pace with technological innovation, the FTC's Section 5 enforcement authority allows it to remain nimble in protecting consumer privacy as technology and consumer expectations evolve over time.

The United States does not require companies to appoint a data protection officer (although specific laws such as the GLBA and HIPAA require companies to designate employees to be responsible for the organisation's mandated information security and privacy programmes). However, it is a best practice to appoint a chief privacy officer and an IT security officer. Most businesses in the United States are required to take reasonable physical, technical and organisational measures to protect the security of sensitive personal information, such as financial or health information. An incident response plan and vendor controls are not generally required under federal laws (other than under the GLBA and HIPAA), although they are best practice in the United States and may be required under some state laws. Regular employee training regarding data security is also recommended. Under the FCC's new Open Internet Order, broadband internet service providers are now also likely to be expected to have incident response plans and vendor controls for data security.

Some states have enacted laws that impose additional security or privacy requirements. For example, Massachusetts regulations require regulated entities to have a comprehensive, written information security programme and vendor security controls, and California requires covered entities to have an online privacy policy with specific features, such as an effective date.

VI DISCOVERY AND DISCLOSURE

Companies may be required under various federal and state laws to produce information to law enforcement and regulatory authorities, and to civil litigation demands. For

27 Bamberger, Kenneth A and Mulligan, Deirdre K, 'Privacy on the Books and on the Ground' (18 November 2011) *Stanford Law Review*, Volume 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Available at http://ssrn.com/abstract=1568385.

example, companies may be ordered to produce information based on federal or state criminal authorities issuing a search warrant, a grand jury subpoena or a trial subpoena, or federal or state regulatory authorities issuing an administrative subpoena. Further, companies could be ordered to produce information upon receiving a civil subpoena in civil litigation.

Such US legal demands may create potential conflicts with data protection or privacy law outside the United States. Companies should consider these possible conflicts when crafting their global privacy and data protection compliance programmes. Consideration should be given to whether US operations require access to European data, such that European data could be considered within the company's lawful control in the United States and thereby subject to production requests irrespective of European blocking statutes.

The United States does not have a blocking statute. Domestic authorities generally support compliance with requests for disclosure from outside the jurisdiction. The principle of comity is respected, but national law and the Federal Rules of Civil Procedure typically trump foreign law.[28]

In a highly significant recent case, the federal court in the Southern District of New York (Manhattan) ruled that Microsoft could be required to transfer customer communications (the contents of emails) stored in Ireland to law enforcement in the United States.[29] The issue in the case concerns whether a search warrant served in the United States could authorise the ex-territorial transfer of customer communications notwithstanding the laws of Ireland and the availability of the Mutual Legal Assistance Treaty process. Microsoft's appeal of the lower court's order requiring it to produce the communications in New York was argued on 9 September 2015. Microsoft's resistance to the US government's search warrant was supported by numerous other communications and tech companies.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Every business in the United States is subject to privacy laws and regulations at the federal level and frequently at the state level. These privacy laws and regulations are actively enforced by federal and state authorities, as well as in private litigation. The Federal Trade Commission, the Executive Branch and state attorneys general also issue policy guidance on a number of general and specific privacy topics.

---

28 *Société Nationale Industrielle Aérospatiale v. US District Court*, 482 U.S. 522, 549 (1987) (requiring a detailed comity analysis balancing domestic and foreign sovereign interests, in particular US discovery interests and foreign blocking statutes). These issues are currently being litigated in a case involving execution of criminal search warrant issued to Microsoft for data stored in its servers located in Ireland. The case is now on appeal following a district court decision obliging Microsoft to produce the data in question.

29 *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp*, 5 F. Supp. 3d 466, appeal pending to the US Court of Appeals for the Second Circuit.

Like many other jurisdictions, the United States does not have a central *de jure* privacy regulator. Instead, a number of authorities – including, principally, the Federal Trade Commission and state consumer protection regulators (usually the state Attorney General) – exercise broad authority to protect privacy. In this sense, the United States has more than 50 *de facto* privacy regulators overseeing companies' information privacy practices. Compliance with the FTC's guidelines and mandates on privacy issues is not necessarily coterminous with the extent of an entity's privacy obligations under federal law – a number of other agencies, bureaus and commissions are endowed with substantive privacy enforcement authority.

Oversight of privacy is by no means exclusively the province of the federal government – state attorneys general have increasingly established themselves in this space, often drawing from authorities and mandates similar to those of the FTC. The plaintiff's bar increasingly exerts its influence, imposing considerable privacy discipline on the conduct of corporations doing business with consumers.

At the federal level, Congress has passed robust laws protecting consumers' sensitive personal information, including health and financial information, information about children, and credit information. At the state level, nearly all 50 states have data breach notification laws on the books,[30] and many state legislatures – notably California[31] – have passed privacy laws that typically affect businesses operating throughout the United States.[32]

Federal Trade Commission

The FTC is the most influential government body that enforces privacy and data protection[33] in the United States.[34] It oversees essentially all business conduct in the country affecting interstate (or international) commerce and individual consumers.[35] Through exercise of powers arising out of Section 5 of the Federal Trade Commission Act, the FTC has taken a leading role in laying out general privacy principles for the

30 See www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

31 See www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

32 See, for example, www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx and www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

33 This discussion refers generally to 'privacy' even though, typically, the subject matter of an FTC action concerns 'data protection' more than privacy. This approach follows the usual vernacular in the United States.

34 See Daniel J Solove & Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 *Columbia L. Rev.* __ (forthcoming 2014) ('It is fair to say that today FTC privacy jurisprudence is the broadest and most influential force on information privacy in the United States – more so than nearly any privacy statute and any common law tort.') available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.

35 See http://export.gov/static/sh_en_FTCLETTERFINAL_Latest_eg_main_018455.pdf.

modern economy. Section 5 charges the FTC with prohibiting 'unfair or deceptive acts or practices in or affecting commerce'.[36] The FTC's jurisdiction spans across borders – Congress has expressly confirmed the FTC's authority to provide redress for harm abroad caused by companies within the United States.[37]

As FTC Commissioner Julie Brill has noted, 'the FTC has become the leading privacy enforcement agency in the United States by using with remarkable ingenuity, the tools at its disposal to prosecute an impressive series of enforcement cases'.[38] Using this authority, the FTC has brought numerous privacy deception and unfairness cases and enforcement actions, including over 100 spam and spyware cases and approximately 60 data security cases.[39]

The FTC has sought and received various forms of relief for privacy related 'wrongs' or bad acts, including injunctive relief, damages, and the increasingly popular practice of consent decrees. Such decrees require companies to unequivocally submit to the ongoing oversight of the FTC and implement controls, audits, and other privacy enhancing processes during a period that can span decades. These enforcement actions have been characterised as shaping a common law of privacy that guides companies' privacy practices.[40]

'Deception' and 'unfairness' effectively cover the gamut of possible privacy-related actions in the marketplace. Unfairness is understood to encompass unexpected information practices, such as inadequate disclosure or actions that a consumer would find 'surprising' in the relevant context. The FTC has taken action against companies for deception when false promises, such as those relating to security procedures that are purportedly in place, have not been honoured or implemented in practice. As part of this new common law of privacy (which has developed quite aggressively in the absence of judicial review), the FTC's enforcement actions include both online and offline consumer privacy practices across a variety of industries, and often target emerging technologies such as the internet of things.

The agency's orders generally provide for ongoing monitoring by the FTC, prohibit further violations of the law, and subject the businesses to substantial financial penalties for order violations. The orders protect all consumers dealing with the business, not just the consumers who complained about the problem. The FTC also has jurisdiction to protect consumers worldwide from practices taking place in the United States – Congress has expressly confirmed the FTC's authority to redress harm abroad caused from within the United States.[41]

---

36 15 U.S.C. Section 45.

37 15 U.S.C. Section 45(a)(4).

38 Commissioner Julie Brill, 'Privacy, Consumer Protection, and Competition', Loyola University Chicago School of Law (27 April 2012), available at www.ftc.gov/speeches/brill/120427loyolasymposium.pdf.

39 See Commissioner Maureen K Ohlhausen, 'Remarks at the Digital Advertising Alliance Summit' (5 June 2013), available at www.ftc.gov/speeches/ohlhausen/130605daasummit.pdf.

40 See, for example, Solove and Harzog, 2014 (see footnote 34, *supra*).

41 15 U.S.C. Section 45(a)(4).

The states

State attorneys general retain powers to prohibit unfair or deceptive trade practices similar to the FTC arising from powers granted by 'unfair or deceptive acts and practices' statutes. Recent privacy events have seen increased cooperation and coordination in enforcement among state attorneys general, whereby multiple states will jointly pursue actions against companies that experience data breaches or other privacy allegations. Coordinated actions among state attorneys general often exact greater penalties from companies than would typically be obtained by a single enforcement authority. In the past two years, several state attorneys general have formally created units charged with the oversight of privacy, including states such as California, Connecticut and Maryland.

The mini-FTC Acts in 43 states and the District of Columbia include a broad prohibition against deception that is enforceable by both consumers and a state agency. In 39 states and the District of Columbia, these statutes include prohibitions against unfair or unconscionable acts, enforceable by consumers and a state agency.

ii Recent enforcement cases

FTC data protection enforcement

The FTC's data protection enforcement has spanned both privacy and security cases and has focused on both large and small companies across a variety of industries. Some illustrative cases are summarised below.

Internet of things

The FTC recently broke new ground by bringing an enforcement action in the emerging field of the 'internet of things'. In September 2013, the FTC announced that it settled a case with TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely. The FTC's complaint charged that the company falsely claimed in numerous product descriptions that its cameras were 'secure'; in reality, the cameras were equipped with faulty software that permitted anyone with the cameras' internet address to watch or listen online. As a result, hundreds of consumers' private camera feeds were made public on the internet. The FTC's order imposes numerous requirements on TRENDnet: a prohibition against misrepresenting the security of its cameras; the establishment of a comprehensive information security programme designed to address security risks; submitting to third-party assessments of its security programmes every two years for the next 20 years; notifying customers of security issues with the cameras and the availability of the software update to correct them; and providing customers with free technical support for the next two years.[42]

The FTC issued its long-awaited report on the internet of things, Internet of Things: Privacy & Security in a Connected World, in January. Two years in the making, the report provides recommendations to companies about protecting consumer privacy and securing customer data created by the new world of sensors and wearables – mainly

42 Press Release, 'FTC Approves Final Order Settling Charges Against TRENDnet, Inc.' (7 February 2014), available at www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

by building security into products and services, minimising data collection, and giving consumers notice and choice about how their data is used. The report considers new statutes to be premature but does suggest that the agency intends to adapt existing authorities under the FTC Act, the Fair Credit Reporting Act and the Children's Online Privacy Protection Act. Republican Commissioner Wright dissented from the report, arguing that the FTC should not issue recommendations and best practices without engaging in a cost-benefit analysis to determine that such measures would, if adopted, improve consumer welfare. Commissioner Wright also suggested that the Commission departed from standard practice by issuing policy recommendations in a workshop report, as such reports typically serve only to 'synthesise the record developed during the proceedings'.

Settlement with TRUSTe

The Federal Trade Commission announced a settlement and consent order with TRUSTe, a 'major provider of privacy certifications for online businesses'. The TRUSTe seal is sold to companies for use on websites to assure consumers of compliance with privacy standards. The FTC claimed that TRUSTe failed to conduct annual recertifications in over 1,000 instances between 2006 and 2013, despite representations that companies using such seals were subject to yearly recertification. The FTC also charged that TRUSTe permitted companies to incorrectly represent it (TRUSTe) as a non-profit corporation after it became a for-profit entity. The consent order subjects TRUSTe to the FTC's jurisdiction and oversight and prohibits such future conduct, and further obligates it to submit detailed information regarding COPPA-related activities to the FTC in an annual filing.

Action under the Restore Shoppers' Confidence Act (ROSCA)

The FTC obtained a federal court restraining order against a group of supplement marketers in its first action under ROSCA. The statute, signed into law in 2010, prohibits marketers from 'charging consumers in an Internet transaction, unless the marketer has clearly disclosed all material terms of the transaction and obtained the consumers' express informed consent', according to the FTC's press release. It prohibits a practice known as 'data pass', which involves sharing a buyer's data to facilitate online purchases of goods or services to a third-party website without the consumer's consent. The ROSCA allegation was one of many in this case, which also includes claims that the defendants violated Section 5 of the FTC Act, the Electronic Funds Transfer Act and the FTC's Telemarketing Sales Rule. The case is *FTC v. Health Formulas, LLC*, D. Nev. 2:14-cv-01649-JAD-GWF.

Router security

The FTC sent Verizon a closing letter informing the company that it had closed its investigation into the alleged failure by Verizon to appropriately secure routers provided to customers. According to the FTC, Verizon regularly shipped routers with the default setting set to the encryption standard 'wired equivalent privacy' (WEP), which had been deprecated by the Institute of Electrical and Electronics Engineers in 2004 because of weaknesses. Despite the FTC's concern about the routers being set to this standard, the

Commission opted to close the case because of the steps Verizon had taken to mitigate the issue. The company ensures that all routers distributed in the future are set to 'wi-fi protected access 2' (WPA2) standard, which replaced WEP; implemented a campaign to tell customers who had received a router set to WEP to update the settings to WPA2; and gave customers with a router set to WEP that is incompatible with the WPA2 setting a chance to upgrade to a newer router. In its letter, the FTC reminded Verizon that data security is an ongoing process that requires constant monitoring and re-evaluation by businesses.

The Verizon letter serves as a good reminder that effective remediation may persuade the FTC not to pursue a law enforcement action. The alleged shortcomings by Verizon are arguably similar to many that have ended in consent decrees between the company involved and the Commission. Importantly, the plan implemented by Verizon addressed potential harm that consumers might suffer. Therefore, it would have been difficult for the FTC to make the necessary showing under the FTC Act that consumers suffer a substantial, avoidable injury.

Online advertising

In December 2012, the FTC announced a settlement with a large online advertising company, Epic Marketplace Inc, that was using 'history sniffing' to secretly and illegally gather data from millions of consumers about their interest in sensitive medical and financial issues, from fertility and incontinence to debt relief and personal bankruptcy. The company would then use this information to send consumers targeted ads. The FTC's order barred the company from continuing to use the history sniffing technology and required it to destroy information that it had gathered unlawfully.[43]

Financial and medical information

In 2009 the FTC settled a case against CVS Caremark (CVS) the largest pharmacy chain in the United States, which had been charged with failing to take reasonable and appropriate security measures to protect the sensitive financial and medical information of its customers and employees, in violation of federal law. Based on its failure to take these measures, CVS was also charged with engaging in unfair and deceptive practices by failing to act in accordance with its claim that 'nothing is more central to our operations than maintaining the privacy of your health information'. The FTC order requires CVS to maintain a comprehensive information security programme; to obtain a biannual audit from an independent professional for the next 20 years; and remain subject to FTC monitoring. In a related settlement with the Department of Health and Human Services, CVS had to develop new policies and practices related to information handling; undergo outside auditing; and pay US$2.25 million to the agency.[44]

43 Press Release, 'FTC Approves Final Order Settling Charges Against Epic Marketplace, Inc.' (19 March 2013), available at www.ftc.gov/news-events/press-releases/2013/03/ftc-approves-final-order-settling-charges-against-epic.

44 Press Release, 'FTC Approves Final Consent Order in Matter of CVS Caremark Corporation' (23 June 2009), available at www.ftc.gov/news-events/press-releases/2009/06/ftc-approve

Safe Harbor enforcement cases

While the future of Safe Harbor is uncertain, the FTC has taken a number of enforcement actions against companies under its Safe Harbor authority, as well as its unfair and deceptive acts and practices authority.[45] The FTC's Safe Harbor cases allege both specific violations of the Safe Harbor privacy principles and false claims of Safe Harbor participation, in which companies continue to represent themselves as Safe Harbor members even when their annual certifications have lapsed. US entities that persistently fail to comply with the Safe Harbor principles will lose the benefits of Safe Harbor participation.[46]

The FTC has continued aggressive enforcement related to Safe Harbor compliance, including, most recently, bringing actions against companies that fail to renew certifications – or who otherwise falsely claimed to be certified. Two more enforcements can now be added to the list: American International Mailing Inc and TES Franchising LLC have both agreed to settle with the FTC for allegedly misleading consumers about their certification under the Swiss and EU Safe Harbor programmes. The FTC alleged that the companies claimed to be in compliance with these programmes when, in fact, their certifications had expired years earlier. The proposed no-fault consent orders would bar both companies from misrepresenting their participation in any government-sponsored privacy or data security programme and would sunset after 20 years.

Mini-FTC Act privacy enforcement cases

In the past few years, state attorneys general have brought a number of enforcement actions pursuant to their authority under their respective states' mini-FTC Acts. Two illustrative examples are summarised below.

Google Street View settlement

Thirty-eight state attorneys general reached a US$7 million settlement with Google over allegations that the company violated people's privacy by collecting wi-fi data as part

s-final-consent-order-matter-cvs-caremark-corporation.

45 See *In the Matter of Myspace LLC*, FTC File No. 102 3058 (2012); *In the Matter of Facebook, Inc*, FTC File No. 092 3184 (2011); *In the Matter of Google Inc*, FTC File No. 102 3136 (2011); *In the Matter of Collectify LLC*, FTC File No. 092 3142 (2009); *In the Matter of Progressive Gaitways LLC*, FTC File No. 092 3141 (2009); *In the Matter of Directors Desk LLC*, FTC File No. 092 3140 (2009); *In the Matter of Onyx Graphics, Inc*, FTC File No. 092 3139 (2009); *In the Matter of ExpatEdge Partners, LLC*, FTC File No. 092 3138 (2009); *In the Matter of World Innovators, Inc*, FTC File No. 092 3137 (2009); and *FTC v. Javian Karnani, and Balls of Kryptonite, LLC*, Civil Action No. 09-CV-5276, FTC File No. 092 3081 (2009).

46 US-EU Safe Harbor Framework: Guide to Self-Certification at 32.

of its Street View activities. Google agreed to train its employees about privacy and confidentiality for at least the next 10 years and to destroy or secure any improperly collected information.[47]

Safari cookie settlements

In July 2013, the New Jersey Attorney General's Office announced a US$1 million settlement with online advertising company PulsePoint concerning allegations that the company bypassed web browser privacy settings to collect information on consumers' online browsing habits to serve millions of online advertisements.[48] In November 2013, 37 states settled an investigation with Google involving essentially the same allegations for US$17 million.[49]

Robocalls

In another recent significant post on its Business Blog, the FTC warned businesses that placing robocalls without first obtaining signed, written consent directly from consumers could subject them to increased scrutiny under the Telemarketing Sales Rule (TSR). In answers to frequently asked questions included in the post, the FTC emphasised that robocalls cannot go to any number, whether on the Do Not Call registry or not, without first obtaining written consent from the consumer – in what some might consider an expansive reading. This consent needs to include the consumer's phone number as well as a clear and conspicuous statement that the consumer gives the specific company, and not a third-party affiliate, permission to make robocalls. The blog entry also reminds entities that if a call list is obtained from a lead generator, that list should still be scrubbed against the Do Not Call registry. The post also cautioned that the TSR's 'business relationship exception' can only be used when the telemarketing calls are live.

iii Private litigation

Privacy rights have long been recognised and protected by common law. The legal scholar William Prosser created a taxonomy of four privacy torts in his 1960 article 'Privacy' and later codified the same in the American Law Institute's Restatement (Second) of Torts. The four actions for which an aggrieved party can bring a civil suit are intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private

47 See, for example, the press release, 'Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data' (12 March 2013), available at www.ct.gov/ag/cwp/view.asp?Q=520518.

48 Press release, 'New Jersey Division of Consumer Affairs Obtains Million-Dollar Settlement With Online Advertising Company Accused of Overriding Consumers' Privacy Settings Without Consent' (25 July 2013), available at http://nj.gov/oag/newsreleases13/pr20130725a.html.

49 Press release, 'A.G. Schneiderman Announces $17 Million Multistate Settlement With Google Over Tracking Of Consumers' (18 November 2013), available at www.ag.ny.gov/press-release/ag-schnetiderman-announces-17-million-multistate-settlement-google-over-tracking.

facts; publicity that places a person in a false light in the public eye; and appropriation of one's name or likeness. These rights protect not only the potential abuse of information, but generally govern its collection and use.

The plaintiff's bar

The plaintiff's bar is highly incentivised to vindicate commercial privacy rights – through consumer class action litigation. The wave of lawsuits that a company faces after being accused in the media of misusing consumer data, being victimised by a hacker or suffering a data breach incident is well known across the country.

Class action plaintiffs reached an agreement to resolve litigation arising from Target's 2013 data breach that compromised the personal information of up to 110 million consumers. Under the $10 million agreement, consumers who can document their losses will be eligible to receive a payment of up to $10,000, and the remainder of the settlement after attorneys' fees will be split evenly among the class. In addition to the payment, the deal requires Target to devote greater efforts towards safeguarding customer data by, for example, appointing a chief information security officer and developing a process for monitoring information security events.

In *Peters v. St Joseph Servs Corp*, the federal District Court for the Southern District of Texas held that the Supreme Court's decision in *Clapper v. Amnesty Int'l USA* compelled the conclusion that an increased risk of identity theft resulting from a data breach is only a speculative future harm, and thus does not qualify as an actual injury for Article III-standing purposes. Under the *Clapper* standard, the plaintiff must at least plausibly establish a 'certainly impending' or 'substantial' risk that he or she will be harmed. In *Peters*, the plaintiff brought a class action for damages arising from a health system data breach. While someone attempted to make purchases using the plaintiff's credit cards, the court held that injury was not imminent, and that the plaintiff failed to establish that the attempted use of her cards was connected to the breach or that injury would be redressed by a favourable ruling.

Role of courts

Courts remain central to defining and reshaping the contours of privacy rights and remedies. This role goes beyond the role of trial courts in adjudicating claims brought by regulators and private parties that seek to protect and define privacy rights and remedies; interest in these issues has been expressed at the highest levels. The Supreme Court has demonstrated recent interest on commercial privacy matters; in a November 2013 dismissal of a petition for certiorari, Chief Justice Roberts noted in dicta what issues the Court might consider when evaluating the fairness of class action remedies brought by plaintiffs challenging a privacy settlement.[50] Consumer protection regulators like the FTC and state attorneys general are becoming increasingly aggressive – both in terms of the scope of enforcement jurisdiction and the stringency of regulator expectations.

50 Statement of Chief Justice Roberts, *Marek v. Lane*, 571 US ___ (2013).

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Foreign organisations can face a federal or state regulatory action or private action if the organisation satisfies normal jurisdictional requirements under US law. Jurisdiction typically requires minimum contacts with or presence in the United States. Additionally, a foreign organisation could be subject to sector-specific laws if the organisation satisfies that law's trigger. For example, if a foreign organisation engages in interstate commerce in the United States, the FTC has jurisdiction. If a foreign organisation is a publicly traded company, the SEC has jurisdiction. If an organisation is a healthcare provider, the Department of Health and Human Services has jurisdiction.

Additionally, foreign organisations must consider the residency of their data subjects. Massachusetts information security regulations apply whenever an organisation processes data of Massachusetts residents. Since Massachusetts was among the first states to enact information security requirements, it has become a *de facto* national standard.

The United States does not have a general data localisation requirement, although certain requirements do exist for government contractors. Though the United States does generally require data localisation, it requires vendor oversight to ensure reasonable standards of data care. A foreign organisation operating in the United States should know they are the responsible party under US law, even if data processing is handled by a vendor outside the United States.

The United States does not have any jurisdictional issues for multinational organisations related to cloud computing, human resources and internal investigations. However, foreign organisations subject to US law should carefully consider how their data network is structured, and ensure they can efficiently respond to international data transfer needs, including for legal process. The United States respects comity but a foreign country's blocking statute does not trump a US legal requirement to produce information.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity has been the focus of intense attention in the United States in recent years and the legal landscape is dynamic and rapidly evolving. Public discourse has tended to conflate distinct legal issues into a single conversation that falls under the blanket term 'cybersecurity'. Cybersecurity law and policy are more accurately described and characterised in distinct buckets primarily consumer or personal information, on the one hand, and critical infrastructure or sensitive corporate data on the other. Of course, the same or similar safeguards provide protection in both contexts.

While the United States does not have an omnibus law that governs data security, an overlapping and comprehensive set of laws enforced by federal and state agencies provides for the security of this information. These information security safeguards for personal and consumer information, as well as data breach notification provisions, are prescribed in the federal GLBA (financial data), HIPAA (healthcare data), and 47 state laws plus the laws of numerous US territories and districts like the District of Columbia (for broad categories of sensitive personal information). The GLBA, HIPAA and Massachusetts

state law[51] provide the most detailed and rigorous information security safeguards. The emergence of the National Institute for Standards and Technology (NIST) cybersecurity framework, as detailed below, is likely to emerge as the predominant framework under which companies undertake to ensure information security.

Forty-seven states have enacted data breach notification laws, which have varying notification thresholds and requirements. These laws generally require that individuals be notified, usually by mail (although alternate notice provisions exist), of incidents in which their personal information has been compromised. These laws usually include a notification trigger involving the compromise of the name of an individual and a second, sensitive data element such as date of birth or credit card account number.

The GLBA Safeguards Rule requires financial institutions to protect the security and confidentiality of their customers' personal information, such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers. The Safeguards Rule requires companies to develop a written information security plan that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

a designate an employee to coordinate its information security programme;

b conduct a risk assessment for risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks;

c design and implement a safeguards programme, and regularly monitor and test it;

d select service providers that can maintain appropriate safeguards, contractually require them to maintain such safeguards, and oversee their handling of customer information; and

e evaluate and adjust the programme in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[52]

The SEC has broad investigative and enforcement powers over public companies that have issued securities that are subject to the Securities Acts, and enforce this authority through the use of a number of statutes, including Sarbanes-Oxley. The SEC has investigated companies that are public issuers that have suffered cybersecurity incidents, including Target, and has considered theories including: (1) that material risks were not appropriately disclosed and reported pursuant to the agency's guidance on how and when to disclose material cybersecurity risk; and (2) that internal controls for financial reporting relating to information security did not adequately capture and reflect the potential risk posed to the accuracy of financial results. The SEC also enforces Regulation S-P, which

51 See Standards for the Protection of Personal Information of Residents of the Commonwealth (of Massachusetts], 201 CMR 17.00, available at www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

52 www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

implements the privacy and security provisions of the GLBA for entities subject to its direct regulatory jurisdiction (such as broker-dealers and investment advisers). In 2015, the SEC and its 'self-regulatory' counterpart FINRA – the Financial Industry Regulatory Authority – have issued guidance and 'sweep' reports regarding the state of data security among broker-dealers and investment advisers.

The Department of Health and Human Services administers the HIPAA Breach Notification Rule, which imposes significant reporting requirements and provides for civil and criminal penalties for the compromise of PHI maintained by entities covered by the statute (covered entities) and their business associates. The HIPAA Security Rule also requires covered entities to maintain appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

In April 2015, the Department of Justice issued its own guide, Best Practices for Victim Response and Reporting of Cyber Incidents.[53] The Department noted concerns about working with law enforcement after suffering a data breach: 'Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harbouring such concerns should not hesitate to contact law enforcement.'

Several states also require companies operating within that state to adhere to information security standards. The most detailed and strict of these laws is the Massachusetts Data Security Regulation, which requires that companies maintain a written information security policy (commonly known as a WISP) that covers technical, administrative and physical controls for the collection of personal information.

In February 2013, President Obama issued Executive Order 13,636, 'Improving Critical Infrastructure Cybersecurity'. This Executive Order directs the Department of Homeland Security to address cybersecurity and minimise risk in the 16 critical infrastructure sectors identified pursuant to Presidential Policy Directive 21.[54] The Order directed the NIST to develop a cybersecurity framework, the first draft of which was released in February 2014. The NIST Cybersecurity Framework provides voluntary guidance to help organisations manage cybersecurity risks, and 'provides a means of expressing cybersecurity requirements to business partners and customers and help identify gaps in an organisation's cybersecurity practices'. While the framework is voluntary and aimed at critical infrastructure, there is an increasing expectation that use of the framework (which is laudably accessible and adaptable) could become a *de facto* requirement for companies holding sensitive consumer or business proprietary data. Companies operating in highly regulated industries such as the defence industrial base, energy sector, healthcare providers, banks subject to detailed examinations by the Federal Financial Institutions Examination Council, or investment firms that are regulated by the Securities and Exchange Commission are subject to detailed cybersecurity standards.

53 Available at www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

54 Available at www.dhs.gov/critical-infrastructure-sectors.

Also, as detailed above, the FTC increasingly plays the role of *de facto* cybersecurity enforcement agency where consumer or personal information is involved. Based on Section 5 of the FTC Act, the Commission has stated that providing reasonable and appropriate information security is required as a 'fair' trade practice. State attorneys general, empowered pursuant to state-level mini-FTC Acts (see Sections VII.i and ii, *supra*) have taken a similar approach. Essentially every major data breach is investigated by the FTC and state attorneys general, and may draw the attention of other regulators, such as the SEC, as well.

X OUTLOOK

There may be more and increasing convergence between US and EU privacy regimes than is commonly believed. Focus on data protection is unquestionably growing throughout the United States, and unlike many other regulatory issues, privacy has not become mired in Democrat–Republican partisan battles. And though the EU often disparages the US approach, in some ways the recent EU privacy proposal cuts some red tape and promotes streamlined EU-wide regulatory approvals. It also focuses more heavily on what has been a priority in the United States, namely information security and data breach notification requirements. The EU's new proposal also seeks to encourage more enforcement and collective redress, like that seen from the FTC and state attorneys general and in private class actions.

No system of data protection anywhere in the world has produced more legal settlements, judgments, consent decrees and, perhaps most importantly, corporate compliance programmes that seek to protect and ensure privacy than the United States. Even though every Member State of the European Union has a data protection authority, they vary greatly in terms of aggressiveness and resources. Indeed, a recent study found that the very 'unpredictability' of FTC's broad mandate proves a stronger incentive to invest in privacy than the European regulators' more siloed mandate.[55]

The FTC noted in recent testimony to Congress that enforcement actions have focused on 'protecting financially distressed consumers from fraud, stopping harmful uses of technology, protecting consumer privacy and data security, prosecuting false or deceptive health claims, and safeguarding children in the marketplace'.[56] The FTC's approach to emerging issues can be informal and inclusive, allowing for productive working relationships that have helped shape the development of products and services in a way that protects consumers while allowing the government to better understand the technology. The use of public meetings and workshops, such as a November 2013 event on the internet of things, to help identify cutting-edge issues raised by technology, is an example of such an approach.[57] The FTC has noted that issues likely to capture their

55 Bamberger and Mulligan, 2011 (see footnote 27, *supra*).

56 Id.

57 Prepared Statement of the Federal Trade Commission on 'The FTC at 100: Where Do We Go From here?' before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade (December 2013).

privacy-related attention in the years ahead include big data, mobile technologies and connected devices, and protection of sensitive data, particularly health information and information that relates to children. Entities known as 'data brokers' have captured the attention of the FTC, and are likely to be targets for future enforcement and oversight. If nothing else, the robust public debate surrounding these issues is indicative of engaged, capable policymakers. Companies have responded to regulation and oversight by expanding privacy leadership functions, redoubling compliance and training efforts, and engaging in proactive and ongoing dialogues with federal and state regulators.

At the same time, cybersecurity continues to be an issue of intense focus for the government and private sector alike. This trend is likely to intensify in the coming years, as technology develops and changes and puts further strain on existing laws. Congressional gridlock has stymied reform on otherwise non-partisan issues, but as the post-Snowden clamour fades, it is possible that legislation will come to pass to enable further collaboration between the private and public sector, and provide clearer reporting and notification requirements, eclipsing the messy state model that exists and is in use today.

Issues related to intellectual property theft are likely to continue to rise to the top of the international diplomacy agenda for the United States as its competitive position risks erosion from China and other such alleged cyber-intruders. Nation-state level interactions on these issue are increasingly likely to include privacy, as the Director of National Intelligence has pinpointed China as the responsible party for the intrusion at the federal Office of Personnel Management that compromised the personal information of millions of US citizens.

Surveillance issues are likely to continue to be a sticking point between US and European counterparts as the explosion of cloud data centres is likely to continue to prove to be a point of tension with regard to requests for information by the United States government.

Investment in protection of computer and communications systems is likely to be a continued regulatory focus, as agencies – and companies – seek to determine and understand how to balance the costs and benefits of imposing information security requirements and reporting. Moreover, implementation of the NIST cybersecurity framework may emerge as a *de facto* requirement for companies. While the broader cybersecurity outlook is unclear, it is certain that intervening factual and technological developments will continue to propel this field to the front of the national consciousness – for reasons related to surveillance, competitiveness and intellectual property theft, or personal security when information is compromised (such as through retail breaches).

Appendix 1

ABOUT THE AUTHORS

CATHERINE VALERIO BARRAD

Sidley Austin LLP

Catherine M Valerio Barrad is a partner in the Los Angeles office of Sidley Austin LLP. She practises primarily in the area of privacy and data protection law, data breach investigations and litigation, cross-border discovery and data transfer issues, and consumer protection litigation including unfair and deceptive practices. She also represents clients in complex civil litigation, consumer class actions and appellate matters.

JILLIAN LEE

Sidley Austin LLP

Jillian Lee is an associate in Sidley Austin's Singapore office and is a member of the complex commercial litigation; white collar: government litigation and investigations; and privacy, data security and information law groups. Her practice focuses on cross-border compliance and investigations, dispute resolution, and regulatory and compliance work involving the life sciences industry, as well as data privacy.

Prior to joining Sidley, Jillian trained at a leading Singapore law firm, where she focused on commercial litigation and insolvency. Jillian also has experience of working in Beijing, Shanghai and the United Kingdom.

Jillian is fluent in English and Mandarin, and is admitted to practise in Singapore.

WILLIAM RM LONG

Sidley Austin LLP

William RM Long is a partner in the London office of Sidley Austin LLP running the EU data protection and privacy practice. He advises international clients on a wide variety of data protection, privacy, cybersecurity, e-commerce and other regulatory matters.

TASHA D MANORANJAN

Sidley Austin LLP

Tasha Manoranjan is an associate in Sidley Austin's Litigation practice in the Washington, DC office, frequently supporting the privacy, data security and information law practice group. Ms Manoranjan earned her law degree at Yale Law School, where she served as the features editor and book reviewer for the *Yale Journal of International Law*, chair of the South Asian Law Students Association and community enrichment chair of the Women of Color Collective. While at Yale, Ms Manoranjan wrote a paper entitled 'Beaten but not Broken: Tamil Women in Sri Lanka', which was subsequently published at 11 *Georgetown Journal of International Affairs* 139 (2010). Ms Manoranjan received her BA, *magna cum laude*, in justice and peace studies from Georgetown University's School of Foreign Service. Before joining Sidley, Ms Manoranjan worked at the Department of Justice Human Rights and Special Prosecutions Section and at an advocacy group working on human rights in Sri Lanka.

VIVEK K MOHAN

Sidley Austin LLP

Vivek K Mohan is an associate with Sidley Austin LLP's privacy, data security and information law group in Washington, DC. Vivek is affiliated with and serves as visiting faculty for the Cyber Security Project at the Harvard Kennedy School, where he spent two years as resident fellow. Vivek has also held a special appointment with the Internet Bureau of the New York State Office of the Attorney General and worked as in-house counsel at the Microsoft Innovation & Policy Center. Vivek holds a JD from Columbia Law School, Columbia University and a BA from the University of California, Berkeley.

TAKAHIRO NONAKA

Sidley Austin Nishikawa Foreign Law Joint Enterprise

Takahiro Nonaka assists foreign companies with compliance matters, including research, negotiating with government officials, conducting internal investigations and drafting internal codes, related to such areas of Japanese law as data privacy, pharmaceuticals, and corporate and labour matters. In high-profile crisis cases, he works with all of the associated investigative agencies and mass media.

Before joining Sidley, he served for nearly 10 years as a district court judge in Tokyo, Nagoya and Kochi, where he presided over cases relating to privacy, disclosure, defamation, labour, corporate, medicine and intellectual property law.

He was seconded to the Embassy of Japan in Washington, DC from 2006 to 2008, where, as a diplomat, he dealt with FCPA and antitrust issues, export controls and legal actions against Japanese companies. He currently handles US antitrust law and FCPA issues, cross-border litigation and international arbitration with the lawyers of Sidley Austin LLP.

Mr Nonaka was also seconded to the human resources department of a leading global Japanese automotive company. He provides clients with strategic services on a wide range of labour issues, including collective bargaining and regulatory correspondence.

He is a member of the practice teams both for FCPA and anti-corruption matters, and for privacy, data security and information law within Sidley Austin LLP.

ALAN CHARLES RAUL

Sidley Austin LLP

Alan Raul is the founder and lead global coordinator of Sidley Austin LLP's highly ranked privacy, data security and information law practice. He represents companies on federal, state and international privacy issues, including global data protection and compliance programmes, data breaches, cybersecurity, consumer protection issues and internet law. Mr Raul's practice involves litigation and acting as counsel in consumer class actions and data breaches, as well as FTC, state attorney general, Department of Justice and other government investigations, enforcement actions and regulation. Mr Raul provides clients with perspective gained from extensive government service. He previously served as vice chairman of the White House Privacy and Civil Liberties Oversight Board, general counsel of the Office of Management and Budget, general counsel of the US Department of Agriculture and associate counsel to the President. He currently serves as a member of the Privacy, Intellectual Property, Technology and Antitrust Litigation Advisory Committee of the National Chamber Litigation Center (affiliated with the US Chamber of Commerce). Mr Raul has also served on the American Bar Association's Cybersecurity Legal Task Force, by appointment of the ABA President. He is a member of the Council on Foreign Relations. Mr Raul holds degrees from Harvard College, Harvard University's Kennedy School of Government and Yale Law School.

GÉRALDINE SCALI

Sidley Austin LLP

Géraldine Scali is a senior associate in the London office of Sidley Austin LLP whose main practice areas are data protection, privacy, cybersecurity, e-commerce and information technology.

YUET MING THAM

Sidley Austin LLP

Yuet Ming Tham is a partner in Sidley Austin's Hong Kong office. She advises international corporations on their legal risks, such as those relating to privacy, data protection and cybersecurity law issues, as well as cross-border compliance and investigations, anti-bribery laws (including FCPA), international trade controls, sanctions, anti-money laundering and dispute resolution.

Prior to joining Sidley, Yuet was the Asia head of the regulatory, compliance and investigations group, and also head of the Asia life sciences group at another international law firm. She has also held roles as a deputy public prosecutor in Singapore and was the Asia-Pacific regional compliance director for Pfizer. During that time, she was responsible for compliance and investigations in Japan, China, Australia, Korea, India, Indonesia, Thailand, Taiwan, Hong Kong, Malaysia, Singapore and the Philippines.

Yuet is named as a leading lawyer in *Chambers Asia-Pacific* in four categories, as well as being recognised in *IFLR1000* and *The Legal 500 – Asia-Pacific*. In 2014, she was the only lawyer awarded the Client Choice award by International Law Office for white-collar crime practice in Hong Kong.

She speaks English, Mandarin, Cantonese and Malay and is admitted to practise in New York, England and Wales, Hong Kong and Singapore.

SIDLEY AUSTIN LLP
39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7888
Fax: +852 2509 3110
yuetming.tham@sidley.com

Sidley Austin Nishikawa Foreign Law Joint Enterprise
Marunouchi Building 23F, 4-1
Marunouchi 2-Chome, Chiyoda-ku
Tokyo 100-6323
Japan
Tel: +81 3 3218 5006
Fax: +81 3 3218 5922
tnonaka@sidley.com

Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3900
Fax: +65 6230 3939
jillian.lee@sidley.com

Woolgate Exchange
25 Basinghall Street
EC2V 5HA
London
United Kingdom
Tel: +44 20 7360 3600
Fax: +44 20 7626 7937
wlong@sidley.com
gscali@sidley.com

555 West Fifth Street
Los Angeles, CA 90013
United States
Tel: +1 213 896 6000
Fax: +1 213 896 6600
cbarrad@sidley.com

1501 K Street, NW
Washington, DC 20005
United States
Tel: +1 202 736 8000
Fax: +1 202 736 8711
araul@sidley.com
tmanoranjan@sidley.com
vivek.mohan@sidley.com

www.sidley.com