ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

German DPA takes action against Safe Harbor firms

Hamburg's DPA is investigating and prepared to issue fines. By **Sascha Kuhn**.

At the end of February, Hamburg's Data Protection Commissioner, Johannes Casper, instituted three proceedings, against subsidiaries of US companies suspected of unlawful transfer of personal data to the United States. Upon completion of the hearings and the proceedings the companies could face fines of up to €300,000 each. The companies had continued using the Safe Harbor Principles of the European Commission (EC) as a legal basis for transferring personal data to their respective parent companies in the US, although this legal

Continued on p.3

EDPS nurtures consumer and DP/competition law cooperation

Giovanni Buttarelli says that closer cooperation between competition, consumer protection and data protection authorities has started. **Laura Linkomies** reports.

Speaking at PL&B's Roundtable in Brussels on 9 March, **Giovanni Buttarelli**, European Data Protection Supervisor (EDPS), said that he is actively working on the dilemmas emerging at the threshold of data protection and antitrust law, complemented by international trade agreements. He said that while it was previously

Continued on p.4

Issue 140 **April 2016**

INTERNATIONAL report

ISSUE NO 140 APRIL 2016

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Hui-ling Chen
Winkler Partners, Taiwan

Lorna Cropper and Kate Pickering
Fieldfisher LLP, UK

Sebastian Golla
Germany

Edward Hasbrouck
Identity Project, US

Kuan Hon
Queen Mary University of London, UK

Sachsa Kuhn
Simmons & Simmons LLP, Germany

Blair Stewart
Privacy Commission, New Zealand

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Safe Harbor no longer safe

A German Land (city state) Data Protection Authority has taken the lead in starting enforcement against three Safe Harbor companies (p.1). Hamburg's DP Commissioner, Dr Johannes Caspar, has not yet declared which firms are involved, but has said that they are large international companies, which should have the legal knowledge and resources to deal with the issue. Caspar is now consulting the affected companies on whether they wish to exercise their right to a hearing. In an interview with *Der Spiegel Online*, the Commissioner said that "There are probably companies that do not seem to take the situations seriously or are willing to accept the risk of fines." Meanwhile, the proposed replacement, the EU-US Privacy Shield, has both supporters and critics (p.6).

On p.23, Stewart Dresner provides an update on the Belgian Facebook case. As a result of many years of close contact from organising conferences and roundtables with them, we are very fortunate to have access to DPAs themselves and learn directly from their staff too. This was the case in Brussels in March, when we organised a Roundtable with the European Data Protection Supervisor, Giovanni Buttarelli. The EDPS is keen to bring data protection, competition and consumer law issues closer together, and is preparing for its important future role under the GDPR as Secretariat to the European Data Protection Board. Read highlights of this meeting from p.1. In addition, the speakers' slides are available to subscribers via *PL&B's* website (p.6).

The EU General Data Protection Regulation continues to be a concern to companies. Data processors will face new responsibilities and will be liable for breaches of the Regulation (p.29). Those using cloud computing need to understand the implications of the Regulation's extra-territorial scope (p.25). But the Regulation also has an influence outside Europe – read on pp.7-9 how the concept of data portability has crept into the law of the Philippines.

The UN Special Rapporteur on Privacy, Professor Joseph Cannataci, has delivered his first Report to the UN Human Rights Council, (pp.10-12) saying he wants to increase awareness and engagement, but what can be achieved without adequate resources? In India, the government is advancing with its plans to introduce a nationwide ID system. There are concerns over data matching which will become easier but remain unregulated (pp.18-20).

Finally, our correspondents in Turkey tell us that the data protection law has been accepted by the Parliament, but the law has not yet been published in its final form in the Official Gazette. As it was not possible to obtain the final version of the law before publication, we will report on this new law in our next issue.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Safe Harbor... from p.1

basis has no longer been available since the judgment of the European Court of Justice (ECJ) dated 6 October 2015.

The ECJ decided in its judgment that the Safe Harbor Principles on the transfer of personal data from the EU to the United States, and based on an EC decision of 2000, did not offer sufficient protection of transferred personal data in the recipient country, i.e. the United States (*PL&B International*, October 2015 p.1). Already in August 2013 (and again in March 2015) the Conference of the Federal as well as the State Data Protection Commissioners in Germany had issued statements that voiced doubts as to whether referring to the Safe Harbor Principles alone supplied sufficient protection of personal data. It stated that, instead, companies intending to transfer data to the US on the grounds of the Safe Harbor Principles had to furnish additional proof of their compliance with an adequate data protection level. It is precisely these reservations that the ECJ chose to be the subject matter of its reasoning. The ECJ had reason to doubt that an adequate data protection level could be ensured in the US in general, even if companies are certified in accordance with the Safe Harbor Principles. In fact, US legislation, under which the protection of personal data cannot be guaranteed even if the participating companies undertake best efforts, must be included as well. This is due to the extensive enabling rules for US authorities, allowing them to gain disproportionate access to the personal data stored by the companies at any time.

The judgment passed by the ECJ did not provide for a transition period to enable converting to other legal bases for data transfers from Europe to the United States. Thus, it has been unlawful to apply the Safe Harbor Principles as a legal basis for transferring personal data to the US. However, many EU DPAs still have a wait-and-see approach.

In a statement concerning the implementation of the judgment, the Hamburg data protection authority (and the other State Data Protection Authorities) granted affected companies a period to be used to otherwise achieve compliance with requirements in relation to international transfers of personal data. The authority set out in detail how the judgment should be implemented. Within this context, all companies that might be affected were contacted. They were to disclose information about the legal basis they used for international data transfer to their respective parent companies. EU standard contractual clauses and Binding Corporate Rules are principles – to be considered in lieu of Safe Harbor Principles – that already exist and are intended for lawful data transfer to the US. Using these two legal grounds might lead to the same problem in respect of the data protection level that existed using the Safe Harbor Principles. However, the judgment failed to state anything in this regard so that these two options are currently regarded by some to be a lawful alternative in transferring data to the US.

The German DPAs agreed not to impose any fines until the Art. 29 Working Party and the various state data protection authorities have reached a concluding legal assessment of these options. Using EU standard contractual clauses or Binding Corporate Rules will continue to be subject to certain special terms, amongst others the obligation to notify the responsible regulatory body when using the Binding Corporate Rules in some German states. However, the EU standard contractual clauses will also require a review according to the European Commission. The EU-US Privacy Shield (*PL&B International*, February 2016 p.1), which is to replace the Safe Harbor Principles, is currently undergoing a legal assessment so that the impact on standard contractual clauses and Binding Corporate Rules is presently unclear.

> International data transfers are a matter of top priority on the agenda of the German DPAs.

German companies may face fines

As announced in the statement issued by the Hamburg Data Protection Authority, at the end of February 2016, the present proceedings were initiated and are currently being considered by the Hamburg DPA. Both the immediate issuing of a statement by the state Data Protection Authorities after the ECJ judgment and the drastic measures taken by the Hamburg Data Protection Commissioner clearly show that international data transfers are a matter of top priority on the agenda of the German DPAs. The systematic procedure and the statements made by the Data Protection Commissioner allow us to perceive that the fines may potentially not be set at the lowest levels possible. The DPAs are authorised to impose fines of up to €300,000 for each infringement. Should companies, after a transition period of almost six months, still be using the model that has become unlawful for transmitting data, the Data Protection Commissioner will have to act on the assumption of intent in their infringing against data privacy laws. Companies were granted a grace period until the end of January 2016 in which no investigations concerning further use of the Safe Harbor Principles were to be carried out. However, carrying out investigations upon expiry of the grace period has been left to the discretion of the separate German state DPAs. Thus, the course of action presently taken by the Hamburg DPA has been foreseeable. This first development should make it clear to companies that they might no longer be safe from being investigated and correspondingly should review their transfers of personal data outside Europe and consider how those transfers are made compliant with EU data protection law.

AUTHOR

Sascha Kuhn is a Partner at Simmons & Simmons, LLP, Düsseldorf and Frankfurt
Email: sascha.kuhn@simmons-simmons.com

EDPS... from p.1

widely thought that data protection was not an issue for competition authorities, two recent court rulings now contribute to a different view. In fact, it is reported that at the beginning of March, the German federal competition authority, the Bundeskartellamt, opened an antitrust investigation into Facebook's activities over alleged unfair user terms.

"Consumer law and data protection law should not exist in silos," Buttarelli said. The EDPS will now revise its preliminary opinion of 2014 on 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy'[1]. In the paper it argued that there is lack of interaction in the development of policies on competition, consumer protection and data protection, and that may have reduced both the effectiveness of competition rules' enforcement and the incentive for developing services which enhance privacy and minimise potential for harm to the consumer.

Buttarelli said that the EDPS is working together with France's Data Protection Authority, the CNIL, and Germany's Bundeskartellamt and that he had visited Paris to discuss these issues with them the previous day. He would welcome closer cooperation between competition, consumer protection and data protection authorities to agree upon a more holistic approach to enforcement. The German and French competition authorities are already cooperating, and a representative of the Bundeskartellamt will visit the EDPS soon to discuss this subject. The EDPS expects to issue an opinion by July.

GDPR implications

Buttarelli said that with the forthcoming EU DP Regulation, we are witnessing a historic moment for data protection. Together with the new framework, the EDPS's role is changing and he is very keen to enhance cooperation with national DPAs and generally increase the visibility of the EDPS. "We are increasingly influential," Buttarelli said. "Data protection is now on the political agenda both at the national and EU level. We try to innovate so that in the future, DPAs would be more transparent and accountable for what they do. This would mean displaying priorities, being more predictable, and measuring performance. The EDPS should lead by example."

The EDPS already assesses implementation of its strategy yearly, and conducts an inventory of every piece of EU hard and soft legislation (such as green papers and communications) and rates them on the scale 'green, yellow, red' depending on their data protection implications. The EDPS strives to promote innovative thinking – how to apply existing DP principles and new EU General Data Protection Regulation (GDPR) aspects such as Privacy by Design. A new aspect of EDPS work is their recently appointed Ethics Advisory Board, which will conduct its research independently and report back to the DPAs' International Conference.

On international relations, Buttarelli said that Europe would like to lead but is now in a minority of countries with data protection laws, citing *PL&B* research (*PL&B International* February 2015 pp. 14-28). But there is a growing interest worldwide to see if the EU succeeds with the GDPR. "The EU aims to adopt the Privacy Shield in early May," Buttarelli revealed.

An Ethics Board has been set up to explore the relationships between human rights, technology, markets and business models in the 21st century.

EDPS future work

The EDPS needs to be selective to be able to be effective - it cannot issue an opinion on everything, Assistant Supervisor, **Wojciech Wiewiórowski**, said. The EDPS speaks with a European voice which can sometimes add to the voice of the national DPAs. The EDPS want to be more modern and less bureaucratic than in the past. One of the objectives is to forge global partnerships. The EDPS will act as Secretariat for the European Data Protection Board (EDPB) which will be established by the GDPR. The Board will prepare opinions in the name of the national EU DPAs, he said.

Wiewiórowski explained that the EU Article 29 Working Party, which will be replaced by the Board, is very active in several fields. Currently, there is consensus so votes are taken only rarely. Subgroups meet almost every week and work on issues such as technology, borders travel, future of privacy, key provisions, e-government, international transfers, financial matters and cooperation. The role of the EDPS will be to coordinate, with the DPAs, supervision of large scale IT systems such as Eurodac, the Visa information system, Schengen, the Customs information system and the Internal Market information system.

Digital ethics and technology

Hielke Hijmans, Special Advisor at EDPS spoke of the route towards new digital ethics. There is an emerging dimension of ethics in data protection – technology should not dictate our values, ethics and rights. Privacy and data protection are increasingly important for protection of human dignity and to participate in society. Information is everywhere and technology companies do not want to be constrained, but innovation should be on an ethical basis. Adherence to the law is not enough, he said.

Hijmans said that the EDPS issued an opinion on ethics in 2015[2], and that an Ethics Board has been set up to explore the relationships between human rights, technology, markets and business models in the 21st century from an ethical perspective. The group, which consist of six people representing fields[3] such as philosophy, economics and social science, started its work in February 2016 and held its

first meeting on 21 March. The EDPS plans to hold a privacy ethics conference in late 2017, and the group is due to complete its work in January 2018. Will ethics be an alternative to law or complementary to law, Hijmans asked. The Board will explore possible ways forward.

Achim Klabunde, Head of IT Policy at the EDPS said that one of the goals of the EDPS is to help data protection to go digital. This will mean promoting privacy enhancing technologies, identifying cross-disciplinary policy solutions and increasing transparency, user control and accountability in big data processing. The EDPS has set up an Internet Privacy Engineering Network, IPEN, and is keen to work with IT developer communities, as well as with academia. The key is to work across disciplines and support Europe-wide discussions, he said.

International transfers

Sophie Louveaux, Head of the Policy and Consultation Unit, and **Gabriela Zanfir**, Legal Officer, spoke about international transfers. Louveaux said that under the GDPR, in the absence of an adequacy decision, companies could transfer personal data based on Binding Corporate Rules and an opinion by the EDPB. Standard contractual clauses adopted by a competent authority and approved by the Commission, as well as support by a favourable opinion by the EDPB under the consistency mechanism would also legitimise transfers. If using the compelling legitimate interest derogation, the number of data subjects affected would have to be quite small, she said, and transfers should not be recurrent. Also the appropriate DPA would have to be informed.

The key message in the Schrems decision invalidating the Safe Harbor (*PL&B International* October 2015 p.1) was that adequate does not mean identical protection. Any interference with fundamental rights must be based on clear and precise rules.The Article 29 DP WP is now assessing the other tools available and we are expecting an opinion soon, she said. The EDPS is preparing an opinion on this question to be issued in late April or the beginning of May.

She said that her personal view is that the GDPR has not changed much for international transfers, and therefore may not attract new adequacy applications. But Wiewiórowski said that some countries are interested in applying for an adequacy declaration. South Korea has applied for an adequacy decision, Japan is considering applying, and Mexico has also expressed interest.

The European Commission would keep its adequacy decisions under review. The Schrems decision made it clear that "adequate" does not mean "identical" but does mean "essentially equivalent."

A question was whether access to data from outside the European Economic Area is considered a transfer? The answer was yes.

The EU-US Privacy Shield would be reviewed in the following order by: the EU Art. 29 DPWP, the EDPS, the Art. 31 Committee (representing the Member States), the European Commission, the European Parliament and the Council of Ministers.

A question was asked whether stored data is subject to EU international transfer provisions? The answer was not if the data is encrypted. If not encrypted, then the issue would need to be reviewed from technical and legal perspectives.

Court of Justice of the EU

Anna Buchta provided the participants with a summary of Court of Justice of the European Union (CJEU) cases that the EDPS has been involved with, or is following as an observer. But how does the EDPS decide when to intervene? It has no direct access to the courts, but needs to monitor the Official Journal just like anyone else, Buchta explained.

Sometimes the EDPS is asked to join a hearing – this is the case in the current proceedings on Passenger Name Record (PNR) data. In the past, the EDPS has intervened, for example in cases that dealt with independence of national data protection authorities, the legal basis of the data retention Directive 2006/24, and PNR data.

Criteria for EDPS involvement include: the importance of a case, whether the EDPS is directly involved, and whether it would contribute to the public good. For example, the EDPS helped Schrems in his case.

By invitation, the EDPS has given evidence with regard to the Digital Rights Ireland case (data retention), and on Schrems (Safe Harbor). Pending cases to follow include:

- C-582/14 Breyer (IP addresses)
- Opinion 1/15 EU-Canada PNR agreement (international transfers) heard on 5 April 2016
- C-203/15 Tele2 Sverige (DRI interpretation: collection vs access/use)
  – Joined with C-698/15 Davis and others (DRI interpretation: UK 'DRIPA')
- C-398/15 Manni (Article 6(e) of Directive 95/46/EC vs commercial registers). This case, inspired by Google Spain, is due to be heard on 12 April 2016.

On the conduct of cases, Buchta said that the language of the CJEU, located in Luxembourg, is French and cases are heard by a bench of three to 13 judges.

Individual rights and consumer protection

Christian D'Cunha, Policy Assistant to Buttarelli and Wiewiórowski, spoke about coherent enforcement of individual rights in the digital single market. For example, the finance and transport industries are now data driven. Interplay between the GDPR and the Unfair Commercial Practices Directive (UCPD) comes into question – is the service "free" if the consumer has to provide personal data (for example, name and email address) in exchange for it?

There are points of intersection between the GDPR and the EU Consumer Rights Directive on transparency for a transaction and similar language. Questions include: What is the deal? How do I agree to the deal? How do I get out of the deal? Is the deal fair? Has the trader acted fairly? Consumer protection agencies already cooperate effectively but there is not much practical interaction between the different enforcement agencies, D'Cunha said.

The EU Charter of Fundamental Rights includes in sequence:

- privacy (Art.7);
- protection of personal data (Art.8); and

- consumer protection (Art.9).

The EU Commission is now working on guidance for the synergy between data protection and consumer legislation – to be issued this summer. While the GDPR will introduce much larger fines, they will still be behind competition law in terms of joint actions, D'Cunha summarised.

The EU's Cross-Border Cooperation Network's priorities are the airlines, the finance industry and the telecommunications industry. Some national level cooperation has taken place, for example, in the Belgian Facebook case (*PL&B International Report* December 2015 p.1). The EDPS aims to issue an opinion by July 2016 on coherent enforcement, and organise a workshop in September.

INFORMATION

PL&B International Report subscribers can gain access to the slides from the EDPS Roundtable by logging into the *PL&B* website and going to hwww.privacylaws.com/Private-Document-Store1/European-Privacy-Officers-Network/European-Data-Protection-Supervisor-Roundtable-9-March-2016/

EU AS CONSTITUTIONAL GUARDIAN

The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: The Story of Article 16 TFEU by Dr Hielke Hijmans, Faculty of Law at the University of Amsterdam and the Faculty of Law and Criminology at the Vrije Universiteit Brussel. This book is the author's doctoral thesis.
He received a joint doctorate from both Universities in 2016.

REFERENCES

1 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

2 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf

3 https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-05-EDPS_Ethics_Advisory_Group_EN.pdf

EU-US Privacy Shield: Conflicting views

The Privacy Shield framework provides an "essentially equivalent" level of protection for personal data transferred from the EU to the US, Hogan Lovells LLP privacy lawyers conclude in their 63-page legal analysis commissioned by the Information Technology Industry Council and DIGITALEUROPE. Published on 31 March, it provides a positive perspective on the Privacy Shield a few days before the European Data Protection Authorities, grouped as the Art. 29 DP Working Party, discuss their opinion in mid-April.

"Whilst we accept that certain aspects of the Privacy Shield framework would benefit from greater clarity, precision and accessibility, we are satisfied that these potential weaknesses do not affect the overall effect of the Privacy Shield framework and the level of privacy and data protection that it affords. In reality the true level of data protection afforded by the Privacy Shield framework will only be demonstrated by its functioning and the practices of its participants," Eduardo Ustaran, Partner at Hogan Lovells said.

For the purposes of a valid adequacy determination by the EU Commission, the Privacy Shield must be able to meet the following specific criteria: unrestricted and independent oversight by the EU DPAs; periodic checks by the EU Commission; effective legal remedies for individuals; and any interference with Articles 7 and 8 (respect for private and family life and the right to the protection of personal data) of the Charter of Fundamental Rights of the European Union must be proportionate and limited to what is strictly necessary.

"We recognise the considerable changes that have taken place in US domestic law since the Snowden revelations in June 2013 about surveillance practices by the US (and other countries). In particular, the introduction of PPD-28, the amendments to FISA, the strengthened role of FISC and other transparency requirements demonstrate the substantial political effort by the US government."

The US has not made progress in adopting an omnibus privacy law, but recently adopted the Judicial Redress Act which provides some privacy rights for EU citizens for data processed by US government.

Criticisms

Several organisations, including European Digital Rights, American Civil Liberties Union (ACLU), EPIC, Digital Rights Ireland and Privacy International have written to the EU Article 29 DP Working Party and the EU Parliament's Committee on Civil Liberties, Justice, and Home Affairs to argue that the proposed Privacy Shield for EU-US data transfers does not provide adequate protection.

The group says that 'EU citizens still cannot be sure what will happen to their data once transferred to the US. Specifically, the US government continues to deny the relevance and application of the internationally-accepted standards of necessity and proportionality in its surveillance operations. In addition, the oversight mechanism established by the Privacy Shield to respond to complaints about US surveillance is not independent, nor does the office come empowered with sufficient authority to initiate investigations or respond adequately to complaints.'

They point out that in order for the Privacy Shield to survive, the US must formally commit to substantial reforms to respect human rights and international law in order to meet the standards set forth by the Court of Justice of the European Union and the Article 29 Working Group. The Privacy Shield contains no such commitment, they say.

- *See www.accessnow.org/cms/assets/uploads/2016/03/Priv-Shield-Coalition-LtrMar2016.pdf*
- *See the full 63-page report at www.hoganlovells.com/files/Uploads/Documents/Privacy%20Shield%20Legal%20Analysis%20by%20Hogan%20Lovells%20(2016-03-31).pdf*

Translating a privacy right to data portability into law

Blair Stewart provides case studies from two regions – the European Union and the Philippines.

There has been debate about the potential usefulness to consumers of 'a right to data portability' for some time. This culminated in 2012 with the European Commission (EC) decision to include the right in the proposed European Union (EU) General Data Protection Regulation (GDPR).

This EU development was mirrored by the inclusion of data portability in the Philippines Data Protection Act 2012. As the Philippines law was enacted and brought into force in 2012 – while the EU instrument merely had the status of a proposal – a commentator has noted that: "Here, an Asian jurisdiction is leading in development of a 'third generation' data privacy principle."[1]

In Europe, as the EC proposal was scrutinised in detail by the European Parliament and the European Council, there has been debate about the practical challenges of implementation of such a right and the pros and cons of doing so. There has also been discussion of whether such a right is best implemented in privacy, consumer protection or competition law.

However, for Europe at least that debate has been resolved – as it was earlier for the Philippines - by the decision announced in December that the decision had finally been taken to enact the right in the new privacy law.

Accordingly, this article does not seek to explore the case for or against a right to data portability but instead takes the opportunity created by the finalisation of the text of the GDPR to look at two available examples of how such a right can be expressed in law.

Philippines Data Protection Act 2012

The Philippines Data Protection Act (DP Act) was signed into law by President Aquino on 15 August 2012 and came into force 15 days after its publication.[2] The text of the law is published online in the Official Gazette.[3]

The policy of the law is declared to be: "… to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected." (DP Act, section 2.)

The right to data portability is contained in section 18 which states: "SEC. 18. Right to Data Portability. – The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer."

It is understood that the law is effectively still not in force as the President has not yet appointed the membership of the National Privacy Commission.[4] A Commission would need to be in place to prescribe formats, standards, modalities and procedures which may be central to the scope and operation of this right in Philippines law.

Although the detail must await prescribed standards, a few observations can be offered:

- **Subject right:** The Philippines establishes data portability as a central data privacy right for subjects alongside more familiar rights such as access and correction.
- **Terminology:** Section 3 defines several relevant terms (namely 'personal information', 'personal information controller' and 'data subject'). The definitions are similar to those found in most domestic privacy laws. The drafting of section 18 is slightly unusual in switching from 'personal information' to 'data' part way through and although the reason for doing so is not obvious the sense remains clear.
- **Obtain/transmit:** Section 18 focuses upon the right to "obtain" a copy of structured electronic data and, unlike the final form of the EU GDPR, is not explicit about conferring a right to require a personal information controller to "transmit" the copy directly to another controller. This is presumably because the text is modelled upon the original 2012 draft of the GDPR proposed by the EC. The drafting of the GDPR altered substantially in this respect during the Trilogue process before being finalised in 2015. However, it may be possible for a creative Commission to prescribe standards to address any potential shortcoming as it is given an express power to specify "procedures for … transfer" for the further use of the data subject.

EU General Data Protection Regulation

The core new right to data portability is contained in Article 18 (set out below). However, before getting to article 18[5] there is reference to the right first in the preamble: "To further strengthen the control over their own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, machine-readable and interoperable format and transmit it to another controller. Data

controllers should be encouraged to develop interoperable formats that enable data portability. This right should apply where the data subject provided the personal data based on his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on another legal ground other than consent or contract. By its very nature this right should not be exercised against controllers processing data in the exercise of their public duties. It should therefore in particular not apply where processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her does not create an obligation for the controllers to adopt or maintain data processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the data should be without prejudice to the rights of other data subjects in accordance with this Regulation. This right should also not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should in particular not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract, to the extent and as long as the data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to obtain that the data is transmitted directly from controller to controller."[6]

This preamble helpfully seeks to explain the policy objectives and explain the right and its limits.

Article 14 of the GDPR is the familiar obligation to provide certain explanations when personal information is collected directly from an individual – the equivalent of the 'notice principle' in the APEC Privacy Framework. This is supplemented by an Article 14a covering circumstances where explanations are required in the context of indirect collection. To ensure fair and transparent processing, both articles include a requirement that individuals be made aware of the new right of data portability.

Article 18 contains the substantive right itself and provides:[7]

"Article 18: Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided, where:
   a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9 (2) or on a contract pursuant to point (b) of Article 6 (1); and
   b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject has the right to [ensure] that the data is transmitted directly from con-troller to controller where technically feasible.
3. The exercise of this right shall be without prejudice to Article 17. The right referred to in paragraph [1] shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph [1] shall not adversely affect the rights and freedoms of others."

As mentioned in relation to the Philippines DP Act, a number a changes were made to this clause between 2012 and 2015. In particular:

- The original first paragraph 1 was deleted and replaced by a first paragraph that transformed the proposed right from a right "to obtain a copy" of data to a "right to receive" data coupled with a "right to transmit … without hindrance" data to another controller and second paragraph that rolls this into a right to have the information sent directly to another controller.
- A new reference is included referring to the relationship to other GDPR rights (namely, the right to erasure) and to rights and freedoms generally.
- Express provision for the EC to specify formats, standards, modalities and procedures has been omitted.[8]

A few observations on the text:

- There are no special terms defined for the purpose of this article.
- There is some obvious overlap between a 'right to receive' and existing subject access rights. The right to non-hindrance in the first paragraph and the right to require direct transmission in the second, seem to be new rights, and certainly strengthen the rights of data subjects, although both could arguably be said to be implied in a broad interpretation (or 'in the spirit of') existing subject access rights.
- There are several novel phrases that will require interpretation including "structured and commonly used and machine readable format", "without hindrance", "technically feasible", "necessary for the performance of a task carried out in the public interest" and "a task carried out in … in the exercise of official authority vested in the controller".
- The potentially competing "rights and freedoms of others" referred to in the fourth paragraph are not made explicit. In an earlier European Council version of the GDPR with marked up proposed changes (21 April 2015) reference was made to the intellectual property rights of processors.

Closing comments

The two case studies show that some economies already see data portability as a right warranting legal status and that privacy law is an appropriate home. There are now legal texts showing that the concept is capable of being rendered into a brief legal text.

Update

The APEC Electronic Commerce Steering Group (ECSG) Data Privacy Subgroup (DPS) meeting in Lima in February received several presentations on the topic of data portability as part of a policy discussion on selected 'next

generation privacy issues'.9 The DPS later adopted a New Zealand proposal to set up a DPS study group to review developments in relation to data portability and report back later in 2016 with any findings or, if warranted, recommendations for further work to be undertaken in 2017. The study group was asked to pay particular attention to the position of consumers in the digital age and the policy interoperability between regional privacy frameworks.

AUTHOR

Blair Stewart is Assistant Privacy Commissioner, New Zealand.

INFORMATION

An edited version of a paper presented to APEC ECSG Data Privacy Subgroup meeting, Lima, February 2016.

REFERENCES

1 Professor Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives, Oxford University Press, 2014, page 346.
2 Understood to be 8 September 2012, source: DLA Piper's Data Protection Laws of the World 2013, March 2013, accessed 11 February 2016: www.edrm.net/resources/data-privacy-protection/data-protection-laws-2013/philippines
3 www.gov.ph/2012/08/15/republic-act-no-10173/
4 Source: Greenleaf, *op cit*, page 337 (as at 2014).
5 The GDPR numbering in this note is taken from the version dated 15 December 2015. It is expected that numbers may change when the regulation is finally issued.
6 See Preamble, clause 55.
7 To make this note easier to follow I have taken the liberty of numbering the clause as it presumably will finally appear. The 15 December working draft's actual numbering goes 2, 2a, 2a, 2aa due to omissions of former clauses 1 and 3 and the interpolation of several new paragraphs. It is not entirely clear whether the internal cross references in the third and fourth paragraphs are intended to refer to paragraph 1 or 2. Obviously, no reliance should be made on this illustrative draft and authoritative EC documentation should be checked when available.
8 It is not clear whether provision for issuing standards etc. is omitted as being considered unnecessary or because the role is to be performed by one of the institutions recognised by the GDPR (such as the supervisory authorities, Data Protection Board or EC) under their general mandates.
9 See Blair Stewart, New Zealand, "Case Studies: Data Portability in the Philippines Data Protection Act and in the new EU General Data Protection Regulation" available at http://mddb.apec.org/Documents/2016/ECSG/DPS-CBPR1/16_ecsg_dps_cbpr_003.pdf ; and Christine Runnegar, ISOC, "Data Portability from Different Interests" available at http://mddb.apec.org/Documents/2016/ECSG/DPS-CBPR1/16_ecsg_dps_cbpr_011.pdf. Malcolm Crompton, IIS, also gave a presentation on consumer perspectives of data portability (no paper available).

US FTC, Canada sign Memo of Understanding

The US Federal Trade Commission (FTC) announced on 24 March that it has signed an agreement with the Canadian Radio-Television and Telecommunications Commission (CRTC) to cooperate on anti-spam initiatives and Do Not Call registry enforcement. The Memorandum of Understanding between the US and Canada enhances information sharing on suspected cross-border Do Not Call registry cases.

"As we see more cross-border fraud, we must often rely on our enforcement partners around the world to help protect US consumers. This agreement will enhance cooperation with the CRTC as we work together to combat illegal telemarketing and spam," said FTC Chairwoman Edith Ramirez.

The CRTC enforces the Canadian Anti-Spam Law, which became effective in 2014. Among other things, the law prohibits the sending of unsolicited commercial email and enables Canadian authorities to provide investigative assistance to foreign enforcement agencies, including the FTC.

• *See www.ftc.gov/news-events/press-releases/2016/03/ftc-signs-memorandum-understanding-canadian-agency-strengthen*

Online reputation: Call for essays

On 18 March, the Privacy Commissioner of Canada, Daniel Therrien, invited contributions on online reputation by 28 April 2016. In January 2016, he released a discussion paper setting out the privacy issues related to online reputation and is now inviting essays in response to the questions posed in the paper. The purpose of asking for essays is to assemble a collection of new and innovative ways to protect reputational privacy, he says.

• *For more information on the procedure for submitting an essay, and the criteria, see www.priv.gc.ca/media/nr-c/2016/an_160318_e.asp and http://blog.priv.gc.ca/index.php/2016/03/18/we-want-to-hear-from-you-about/*

***PL&B* CONFERENCE: DANIEL THERRIEN**

PL&B is pleased to announce that the Privacy Commissioner of Canada, Daniel Therrien, will speak at *Great Expectations*, Privacy Laws & Business's 29th Annual International Conference, 4-6 July 2016 at St. John's College, Cambridge.
See a two-minute video trailer at www.privacylaws.com/annualconference
An updated list of speakers is at www.privacylaws.com/speakers

UN privacy rapporteur sets high standards but lacks resources

The United Nations appointed a part-time Rapporteur on Privacy last year. **Graham Greenleaf** reports.

The UN Special Rapporteur on Privacy (SRP), Professor Joseph Cannataci, has delivered his first Report[1] to the UN Human Rights Council, eight months into his three-year term.[2] One of the strengths of this Report is that it gives a reasonably clear idea of the SRP's views on what are the greatest threats to the global protection of privacy, and his initial responses to those threats. As well as outlining and discussing those views, this article also discusses how he highlights the fundamental role of the purpose-specification principle in data privacy protection, and his approach to the role of international agreements on privacy. It concludes by looking at the resources available to a UN Special Rapporteur. Quotations are from the SRP's Report except where indicated otherwise.

'The beginning of the judicial end for mass surveillance'

The SRP uses these uncompromising terms to characterise the decision of the Court of Justice of the European Union (ECJ) in the *Schrems* decision (*PL&B International*, October 2015, p.1), stressing what he regards as the Court's "precedent-confirming (and setting)" statement that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the [EU] Charter."

He argues that any ambiguity in the words "access on a generalised basis" is "at least partially dispelled" by the decision of the European Court of Human Rights (ECtHR) in its December 2015 decision in *Zakharov v Russia*[3] where the Grand Chamber of the Court held unanimously that the Russian system of secret interception of mobile telephone communications was a violation of Article 8 of the European Convention on Human Rights. In the Court's words "the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorization," creating a "particularly great" need for safeguards. The SRP sees this as "the test against which all existing and new proposed legislation about surveillance in any European country must be measured," and in that sense complementing what was required in *Schrems*. He therefore presents the two highest judicial authorities relevant to member states of the EU as establishing compatible authorities on what can be seen as the key issue of his mandate, mass surveillance. *Zakharov* is also seen as particularly interesting because the complainants were not required to show that they had been the subject of secret surveillance; it was sufficient that a secret surveillance measure existed. This approach has been rejected by US courts.

> The SRP is clearly looking to the courts of Europe to set the benchmarks for the limitations on mass surveillance

Following this approach, Cannataci argues that the UK government's proposals for the Investigatory Powers Bill "*prima facie* fail the benchmarks set by the ECJ in Schrems and the ECtHR in Zakharov". Rather than see the UK's legislation before either of these courts, the SRP encourages the UK government to "set a good example and step back from taking disproportionate measures" particularly because of "the huge influence that UK legislation still has in over 25% of the UN's members states that still form part of the Commonwealth, as well as its proud tradition as a democracy which was one of the founders of leading regional human rights bodies such as the Council of Europe."

The SRP is clearly looking to the courts of Europe to set the benchmarks for the limitations on mass surveillance which might then form the basis for a global standard.

'First small steps towards cyberpeace?' A related positive area perceived by the SRP comes from the September 2015 discussions and agreement between the US and China that "neither government would support or conduct cyber-enabled theft of intellectual property". The SRP sees "cyberpeace" as having, as well as this economic dimension, the avoidance of sabotage and warfare, and the avoidance of surveillance. "In this sense at least, privacy protection is also part of the Cyberpeace movement." It is a new perspective on data protection, but will it gain adherents?

One element of "cyberpeace" of which he clearly approves is the "wise restraint" shown by the Netherlands government in its January 2016 announcement that it formally opposes the introduction of backdoors in encryption products.[4] Concerning the then ongoing *Apple v FBI* case over whether Apple could be forced to develop software to defeat security features on its phones, the SRP agreed with the separate statement by the UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein, arguing that "A successful case against Apple in the US will set a precedent that may make it impossible for Apple or any other

major international IT company to safeguard their clients' privacy anywhere in the world."[5]

Genetics, biometrics and privacy

He notes disturbing rapid increases in the use of DNA databases: "approximately 25% of the UN's member states, have implemented national criminal offender DNA … database programs"; civilian uses, such as for ID cards and immigration are expanding exponentially; "it is likely that we will see the first country move forward with a citizen-wide DNA database"; and insurance uses "will cause many citizens to voluntarily submit their full human genomes to the health care industry" (although we would have to describe this last as 'quasi-voluntary' at best). Closely related is "a huge surge in interest in using all forms of biometrics for a variety of purposes ranging from law enforcement to personal access to mobile devices", including "voice and speaker identification, retina scans, gait recognition, face recognition, fingerprint and sub-cutaneous fingerprint technology." This is one area of the Report where the SRP holds his cards close: the areas of concern are stated clearly enough, but policies remain unstated other than to continue engagement with all parties.

Anonymisation, Open Data and Big Data analytics

Despite his concerns about State mass surveillance, the SRP regards corporate use of personal data as a comparable threat: "In the early days of digital computers, one of the main concerns was the use of personal data by the state and the state's abilities to correlate data held in various sources to form a detailed picture of an individual's activities and assets. In 2016 it would seem that much more data is held on the individual by corporations than that held by the state." Not only has the data available for profiling increased by an order of magnitude in 25 years but there is also "not enough evidence available to properly assess the risk inherent in purportedly anonymised data which can be reverse engineered in a way such to be linked to an identified or identifiable individual." The reversibility of supposed de-identification/anonymisation is a major theme of the Report. He takes a very skeptical view of the 'Open Data' movement and its demands for open access to public data sets, because they then become susceptible to Big Data analytics. "It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide."

Back to basics: The purpose-specification principle: The principle that Open Data and Big Data both threaten is the purpose-specification principle. "Put simply, personal data should be collected, used, stored and re-used for a specified legitimate purpose or for a compatible purpose" – and then deleted permanently. It "is not something invented by Europeans", having first appeared in a seminal US government report in the early 1970s, stated as "There must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent".[6] He briefly traces the principle through the OECD privacy Guidelines of 1980, the Council of Europe data protection Convention 108 of 1981, and through to the EU Directive of 1995 and the GDPR now being finalised (where he considers it is not diminished). He concludes that "it is not as if the European Union appears ready to abandon the principle of purpose limitation" (he does not add 'even if the US has forgotten it'), indicating he is not likely to abandon it either, and that it is the line in the sand with which both Open Data and Big Data must deal.

Cannataci's professorial background may show, but it is very valuable for him to state at the outset that this is the fundamental principle for which his office stands.

Carrots and sticks: The SRP considers that personal data businesses require penalties which threaten their business models before they are likely to respond to privacy interests: "The vast revenues derived from the monetisation of personal data … mean that the incentive for changing the business model simply on account of privacy concerns is not very high. Indeed, it was only when recently risks to privacy threatened the income potential of the business model that some corporations took a stricter more privacy-friendly approach." This is hard-line but realistic: penalties must threaten business viability before businesses will respond.

The role of international privacy agreements

The world's data protection authorities, at their annual meeting a few months after the SRP's appointment, resolved[7] (apart from desiring mutual cooperation) to reaffirm their call in 2013 for an additional protocol to Article 17 (the existing brief privacy provision) of the International Covenant on Civil and Political Rights (ICPPR). The conference then called upon the Rapporteur "to promote the start of negotiations on such a protocol within his first mandate". This proposed protocol would set out a more detailed set of data privacy rights based upon the UN Human Rights Committee's General Comment No. 16 interpreting ICCPR article 17, "in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law". The US FTC abstained in 2013 and 2015 from the resolution "which relates to matters outside its jurisdiction".

One of the advantages of such a Protocol (not discussed in the Report) is that it is open to unilateral adoption by any of the 169 UN members that have ratified the ICCPR, without requirements of approval ('adequacy', accession etc.) by other countries. However, it does carry with it the requirement that a country submit to periodic review by the Human Rights Council of the extent to which it has complied with its obligations. Depending on how the new Protocol is framed, it could also carry with it an obligation to allow "communications" (complaints) from citizens of the country to the Council, if they did not meet the standards of the Protocol.

The SRP identifies the updating of existing international legal instruments as "an essential starting point". Although he notes that there "appears to be a consensus among several

stakeholders" that a new protocol to ICCPR Article 17 is desirable, he considers that the timing of this might depend on the adoption or a new international agreement on other privacy-related issues such as jurisdiction and territoriality in cyberspace. However, he does not envisage "one new global all-encompassing international convention covering all of privacy or Internet governance" but rather "incremental growth of international law and thus the clarification and eventually the extension of existing legal instruments as well as even, in the mid to long term, the development of entirely new legal instruments."

One existing agreement that receives little attention in the Report is Council of Europe data protection Convention 108, although it is currently being slowly 'globalised'.[8] However, the SRP is meeting the Chairperson of its Consultative Committee on Data Protection (T-PD).

What is the UN's ongoing role in data privacy?

Subject to his resource and time constraints, the SRP has embarked on a "Ten Point Action plan" of increasing awareness and engagement, detailed in the Report. Its headings are: (a) Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect; (b) Increasing awareness; (c) The creation of a structured, on-going dialogue about privacy; d) A comprehensive approach to legal, procedural and operational safeguards and remedies; (e) A renewed emphasis on technical safeguards; (f) A specially-focused dialogue with the corporate world; (g) Promoting national and regional developments in privacy-protection mechanisms; (h) Harnessing the energy and influence of civil society; (i) Cyberspace, Cyber-privacy, Cyber-espionage, Cyberwar and Cyberpeace; and (j) Investing further in International Law.

Few outsiders to the UN system probably realise that the prestigious positions of Special Rapporteurs come without any resources to carry out their daunting tasks: no staff, not even a travel budget (except perhaps when summonsed to the Human Rights Council). The Report explains this in detail, and that it is vital to obtain "extra mural funding outside UN sources". So far, academic sources have produced one full-time post-doctoral researcher, much assistance from academia and NGOs (including some part-time volunteers), and negotiations with DPAs which may generate some seconded staff. Negotiations with governments and the private sector are intended to follow. This "first SRP" is actively pursuing the building up of such capacity "to ensure sustainability of work on privacy protection". This has the potential to benefit this SRP, but also his successors if this mandate is renewed. However, it has be to be borne in mind at all times, when considering what a SRP achieves, what resources they did or did not obtain, and the source of those resources.

REFERENCES

1 United Nations Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, Human Rights Council, Thirty-first session, 8 March 2016.
2 For background to the appointment, see Graham Greenleaf 'The UN Special Rapporteur: Advancing a Global Privacy Treaty?' *Privacy Laws & Business International Report*, October 2015, pp. 7-9.
3 Roman Zakharov v Russia [2015] ECHR 1065 (4 December 2015) www.bailii.org/eu/cases/ECHR/2015/1065.html
4 Tweede Kamer, 'Kabinetsstandpunt encryptie' 4 January 2016 www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015
5 UNHCHR Media release 'Apple-FBI case could have serious global ramifications for human rights: Zeid' 4 March 2016 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E
6 Department of Health, Education and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, U S Govt. Printing Office, Washington USA 1973 at p. 41.
7 37th International Conference of Data Protection and Privacy Commissioners' Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy, Amsterdam, 27 October 2015.
8 Graham Greenleaf 'International DP agreements after the GDPR and Schrems' , *PL&B International Report*, February 2016, pp. 12-15.

Merck and Capgemini achieve BCRs

US based Merck & Co. Inc. (Merck) Binding Corporate Rules (BCR) were approved on 1 March. The company's lead authority was the Belgian DPA. Merck is the first company to complete BCRs having, in October 2013, first achieved APEC Cross Border Privacy Rules (CBPR) certification with TRUSTe.

Capgemini's BCRs were approved on 15 March by the CNIL, France's DPA. The BCRs' dual certification applies both to controller and processor data thus covering both its own personal data and the personal data of its clients.

"BCRs are a key business differentiator for Capgemini as we are now one of the very few global players in our industry to have BCRs approved both as data controller and data processor. By putting in place the appropriate policies, security measures, awareness campaigns and audit programs, Capgemini is offering its clients the highest standards currently available in the market," said Paul Hermelin, Chairman and CEO of the Capgemini Group.

• *82 companies have now had BCRs accepted. See http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm*
On Gapgemini, see www.uk.capgemini.com/news/news/capgemini-announces-its-binding-corporate-rules-certification-a-global-data-privacy

Taiwan amends and fully implements its data protection law

Taiwan's law has been called the world's strictest privacy law. **Hui-ling Chen** reports on the changes for consent and sensitive data that now relax the rules somewhat.

After six years of delayed full implementation, Taiwan's second generation data protection law finally came completely into force on 15 March 2016 following amendments to the Personal Information Protection Act ("PIPA") enacted in December 2015[1].

The amendments resulted in a final but weakened version of the PIPA. Key changes include increasing the number of exceptions to permit the processing of special (sensitive) categories of sensitive data from four to six including consent (§6), a relaxation of consent requirements to process ordinary personal data (§7), and decriminalization of violations of PIPA where the offence was committed without specific unlawful or harmful intent (§41).

Article 1 of the PIPA sets two competing policy goals for the regulation of personal data in Taiwan: protection of privacy and reasonable use. From an internal perspective, the amendments to the PIPA mark a rebalancing of the PIPA away from strict protection of privacy toward reasonable use. From a comparative perspective, the amendments represent not only Taiwan's retreat to a weaker version of second generation data privacy standards, but also Taiwan's first tentative steps toward transplanting the EU's General Data Protection Regulation into domestic law.

The following discussion of Taiwan PIPA's substance focuses primarily on the implementation of sensitive data protections with the details of how Taiwan defines sensitive data and the new exceptions permitting processing of sensitive data including consent. That discussion is followed by summaries of the relaxed consent requirements for ordinary personal data, changes to criminal liability under PIPA, and the notice requirement for personal data received from third parties pre-PIPA.

Sensitive Data

The principle that special protection should be afforded to special categories of data has been identified as a second generation 'European' principle of data privacy law. [2]

Taiwan's legislature enacted the sensitive data protection principle in Article 6 of PIPA in 2010, citing Directive 95/46/EC, Germany's Federal Data Protection Act, and Austria's Federal Act concerning the Protection of Personal Data as models. However, Article 6 was not put into force in 2012. As a result, Taiwan's data protection regime effectively lacked special protection for sensitive data until now.

PIPA's definition of sensitive data

As amended and currently in force, sensitive data under the PIPA is data pertaining to a data subject's health, sexuality, and criminal history. In particular, "medical records, medical treatment, sexuality, physical examinations, and criminal records" may not be collected, processed, or used unless a permitted exception applies (PIPA §6). According to the accompanying legislative documentation, these definitions are based on what is described as Taiwan's 'national conditions' and the 'people's understanding' of which data is sensitive.

> Taiwan's data protection regime effectively lacked special protection for sensitive data until now.

In any event, the scope of sensitive data under the PIPA is narrower than that found in its European forerunners and 95/46/EC because trade union membership, racial and ethnic data, and religious and philosophical views are not sensitive categories of personal data under the PIPA.

As a result, it can be said that Taiwan's implementation of the sensitive data protection principle is weaker than its European models starting with its initial definition of sensitive data.

Processing of sensitive data: original permitted exceptions

As originally enacted in 2010, PIPA's narrow definition of sensitive data was combined with a relatively strict set of four exceptions permitting processing of sensitive data:

1. where expressly provided by other law,
2. where there is a statutory duty or obligation to collect, process, or use the sensitive personal data,
3. where there is a voluntary disclosure by the data subject or other lawful disclosure, and
4. for health and criminological research. PIPA §6(1)(1)-(4).

Notably, the data subject's consent was not a permitted exception under PIPA as originally enacted. In contrast, Germany and Austria's data protection laws both permit processing of sensitive data with the data subject's consent. In this sense, PIPA, as originally enacted, was stronger than the European models that Taiwan followed.

As a result, Taiwan's executive branch became concerned that Article 6 of PIPA as enacted in 2010 was "overly strict". Indeed, a leading Taiwanese business magazine somewhat hyperbolically called it the "world's strictest privacy law." These concerns caused the executive branch to delay implementation of PIPA as a whole for two years. Although the PIPA was finally implemented in 2012, Article 6 (and 54,

about data processors informing individuals about their first use of personal data) was not put into force on grounds of administrative impracticability.

New permitted exceptions: assistance and consent

In December of last year, the legislature enacted a new version of Article 6 that added two new exceptions permitting the processing of sensitive data:

1. Collection, processing, and use as necessary to assist public agencies in the exercise of their official duties and private sector actors in meeting their statutory obligations, and
2. Collection, processing, and use of sensitive data with written consent of the data subject. PIPA §6(1)(5)-(6).

The assistance exception

The assistance exception is probably best understood as a scaled-back version of a public interest exception proposed by the Ministry of Justice but ultimately rejected by the legislature. In its general explanation of the proposed public interest exception, the Ministry cited Article 9 of the EU's General Data Protection Regulation and provided two illustrative examples of circumstances where the collection, processing and use of sensitive data was said to be justified on public interests grounds: schools that are required to accommodate children with rare illnesses and criminal background checks on candidates for elected public office. According to the Ministry, schools with students suffering from rare diseases would need to provide medical data to outside service providers (i.e. a use of sensitive data) when schools offered extracurricular activities off campus. Similarly, law enforcement would need to provide (another use of) criminal records to election officials for background check purposes.

Both of these examples involve the statutory duties of public agencies and are thus covered by the assistance exception as adopted and now in force. This exception is narrower than the public interest exception since it can be invoked only if the public agency or private actor to be assisted has a clear statutory duty or obligation. As a result, the assistance exception is probably best understood as being complementary to the official duty/statutory obligation exception of PIPA §6(1)(2). Under the official duty/statutory obligation, one public agency has grounds to request sensitive personal data such as medical or criminal records from another public agency. Conversely, the public agency receiving the request now has grounds under the new assistance exception to provide the requested information.

Consent exception

The rationale for the new written consent exception for sensitive data is two-fold. First, leading European jurisdictions such as Austria and Germany permit processing of sensitive personal data with the data subject's consent. Second, the Ministry of Justice argued that consent exception was necessary to invest the data subject with the right to "autonomous control" over personal data including special categories of personal data. According to the Ministry, Taiwan's Constitutional Court has identified this right to autonomous control as one of the bundle of rights that constitute the constitutional right of privacy in Taiwan. Consent from a data subject to process sensitive data must be written and is invalid if it exceeds the "necessary scope" of the data processing purpose or if it is obtained under duress.

Consent easier to obtain

Article 7 of PIPA as revised now makes it easier for public and private sector data processors to obtain the data subject's consent to collect, process, and use ordinary personal data. First, consent to collect or process such personal data is no longer required to be written §7(1). Second, consent to use personal data for extended purposes no longer needs to be written §7(2). Third, a presumption of consent by the data subject to collection or processing arises if the data subject does not refuse consent after the data processor has informed the data subject of:

1. The purpose of the intended collection, processing, or use of personal data; and
2. The data subject's rights to access, correction, and deletion of his or her personal data §7(3).

However, no presumption of consent arises in the context of notice of an extended use. Consent to extended use must be an independent affirmation of assent to the proposed extended use that is valid only if the data subject has been informed of the new purpose of use. The data collector has the burden of proof to show that the data subject has consented [PIPA §7(3)]. The concern here and elsewhere in the December 2015 PIPA amendments regarding the nature and quality of consent echoes that regarding Article 7 of the draft EU General Data Protection Regulation.

Criminal Liability

After implementation of the PIPA, it quickly became apparent that minor personal disputes between private citizens were leading to convictions under the first paragraph of Article 41, which formerly provided that a person who violated any of the main provisions of the PIPA (such as collecting, processing and using personal data without proper consent or another applicable exception) without any specific criminal intent could be sentenced to up to two years of imprisonment. Article 41 has now been amended to eliminate criminal liability for violations of PIPA without specific criminal intent. Under Article 41 as amended and in force, only enumerated violations of PIPA committed with unlawful purpose or to harm the rights or interests of another are punishable with imprisonment of up to five years and, optionally, a fine of up to NT$1 million (around US$30,000).

Notice for personal data from third parties

Finally it should be noted that Article 54 amendment and coming into force requires data processors with personal data obtained from third parties (prior to December 2015) to notify data subjects prior to the first use of the personal data after 15 March 2016.

Conclusions

Taiwan's 2015 amendments to PIPA have resulted in the implementation of a more complete second generation data protection law since protections for sensitive data are now finally in place. However, Taiwan's second generation data protection regime has been lightly enforced due to the lack of a data protection authority.

Now light enforcement has been combined with additional exceptions to the processing of sensitive data and relaxed consent requirements for ordinary personal data. In general, Taiwan is committed to adopting international standards but is doing so cautiously without trying to lead or innovate. Its data protection law has proved to be no exception to this go-slow approach.

AUTHOR

Hui-ling Chen is a Partner at Winkler Partners and supervises all Taiwan litigation.
Email: hchen@winklerpartners.com

REFERENCES

1 PIPA took effect in 2012. See *PL&B Int*, Feb. 2014, p.16 for analysis 'One year on' by the author, and *PL&B Int* Dec. 2011 on proposed changes to Taiwan's data privacy law.
2 Graham Greenleaf: *Asian Data Privacy Laws* (2014)

German consumer law creates new DP rights

Germany's "Act to Improve the Civil Enforcement of Consumer Protection Provisions of Data Protection Law", which was published on 17 February, entered into force on 24 February 2016, provides a possibility for consumer protection associations to file privacy cases in court on behalf of individuals.

Not-for-profit consumer protection organisations may start court action in cases of data protection violations in the fields of advertising and marketing, opinion research, creating personal profiles and selling personal data (including address details) to third parties. The courts may not award damages in these cases but it is thought that negative publicity may prove a powerful punishment.

Importantly, the law states that consumer organisations cannot make claims against violations of international data transfer rules until 30 September 2016.

• *See copy of the law (in German) at www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*[%40attr_id%3D%27bgbl116s0233.pdf%27]__1456238476520*

CNIL fines Google over 'Right to be Forgotten'

France's Data Protection Authority, the CNIL, on 10 March, fined Google €100,000 for its alleged failure to provide an efficient de-listing service.

In February, Google said that it would apply Right to be Forgotten (RTBF) to all of the search engine's domains when the search is conducted in Europe. But the CNIL requested that delisting be applied to the entire search engine – including requests from all of its website domains.

The CNIL said at the time of the March judgement: "The Google search engine service represents a single processing operation and the different geographic extensions (".fr", ".es", ".com", etc.) cannot be considered separate processing operations. The company originally operated its service using the '.com' extension, then created extensions as time went by to provide a service adapted to each country's national language."

"This means that, for people residing in France to effectively exercise their right to be delisted, in accordance with the Court of Justice of the European Union's decision, the delisting must be applied to the entire processing operation, i.e. to all of the search engine's extensions."

"Contrary to Google's statements, applying delisting to all of the extensions does not curtail freedom of expression insofar as it does not entail any deletion of content from the Internet. At a physical person's request, it simply removes any links to website pages from the list of search results generated by running a search on the person's first name and surname. These pages can still be accessed when the search is performed using other terms."

Google proposed to filter results based on the geographic origin of the person performing the search. This means that people using the search engine from the same country as the complainant's country do not access the delisted result any more. However, the CNIL said that personal or professional contacts living outside Europe can still access the delisted search result linking to content that may infringe the privacy of the person concerned.

• *See https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google*

Morocco to host next DPAs' conference

The Moroccan Data Protection Authority will host the DPAs' international conference from 17-21 October 2016, with the public session on 20-21 October. The DPA aims to offer "a point of entry of the culture of privacy and personal data protection to new countries, especially in the Arab, Muslim and African regions."

• *The secretariat of the DPAs' international conference is at https://icdppc.org/*

Germany criminalises trading 'stolen' data via the Internet

Sebastian Golla analyses the new criminal offence of handling stolen data under the German Criminal Code and its implications for German Information Law.

In March 2012 the Ministry of Justice of the state of Hessen proposed a new criminal offence, Handling Stolen Data (*Datenhehlerei*). Subsequently, several drafts for a new provision were presented and discussed. On 16 October 2015 the German Bundestag passed an amendment to the Criminal Code that introduced the criminal offence of Handling Stolen Data together with a new Data Retention Law. The amendments entered into force on 18 December 2015.

The provision reads as follows:[1]

"Section 202d – Handling Stolen Data

(1) Whoever acquires for himself or for another, supplies to another, disseminates or makes otherwise accessible data (Section 202a (2)), which is not generally accessible and that another has acquired by an unlawful act, with the intent of enriching himself or another or of harming another, shall be liable to imprisonment not exceeding three years or a fine.

(2) The penalty must not be more severe than that for the unlawful act by which the data was acquired.

(3) Subsection (1) does not apply to actions which exclusively aim at fulfilling lawful official or professional duties. These particularly include

1. those actions by public officials or their representatives by means of which data is supplied exclusively for utilisation in proceedings in tax matters, criminal proceedings or summary fine proceedings and
2. those professional actions by a person listed under Section 53 (1) 1st sentence No 5 of the Code of Criminal Procedure by means of which data is received, processed or published."

Objective of the provision

The objective of the provision is to criminalise the trading of "stolen" data via the Internet or "Darknet" services and platforms. The legislative documents[2] describe a "black market" for stolen data with three types of perpetrators: Those who unlawfully acquire data in the first place via Data Espionage or other unlawful acts, those who trade the data, and those who buy data to commit other crimes (such as Computer Fraud by withdrawing money from bank accounts). In particular, the criminal offence of Handling Stolen Data is directed toward the second group of "black market traders" who neither commit prior crimes to acquire stolen data nor use the data to commit subsequent crimes. According to the Draft, this form of handling data is not adequately covered by the existing provisions of Criminal Law.

Object of the crime

The object of the crime is all data which:

- is stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable (requirement from Section 202a (2)),
- is not generally accessible (e.g. not already published), and
- has been acquired by an unlawful act.

The scope of the offence is not limited to personal data. The offence can apply to data related to legal entities as well as to other types of unpublished data (such as machine data or random notes). The offence can apply even in the event that there is no material interest in the data. As a consequence, the handling of information which is not considered to be a private, business or a trade secret under German Law could be considered a criminal offence under certain circumstances. In this respect, the provision expands the overall legal protection of information and creates new liability risks.

Moreover, the requirement that the data be acquired as a result of an unlawful act allows for a broad interpretation. An unlawful act can be any criminal offence which leads to the acquisition of data, e.g. the theft of a hard drive or a coercion which leads to the disclosure of data. Unlike the offence of Handling Stolen Goods (Section 259 German Criminal Code), which is limited to "property that another has stolen or otherwise acquired by an unlawful act directed against the property of another" (such as theft, fraud, blackmail, burglary or robbery), unlawful acts under Section 202d do not have to be directed against a particular legal interest.

Criminal actions

As relevant criminal actions Section 202d name:

- the acquisition,
- supply,
- dissemination, and
- the making available of data.

These actions are similar to the actions punishable as Data Espionage under Section 202a German Criminal Code, which only applies to data specifically protected against unauthorised access. In particular, the acquisition (for oneself or for another person) of data covers a wide range of actions including the collection and disclosure of data. This also includes the actions (redundantly) described as supply and dissemination of data.

Additionally, the described actions are only punishable if taken with the intent of personal enrichment, of enriching another or of harming another. This requirement appears in a similar form in Section 203 (5) German Criminal Code (as a qualification to the offence of Violation of Private Secrets) and Section 44 (1) Federal Data Protection Act. While the harming of another includes both material harm (damage of property) and immaterial harm (e.g. indignity), the intent of enrichment requires the

existence or possibility of a direct monetary profit from handling the data.

Limitation of scope

According to Subsection (3), actions which exclusively aim at fulfilling lawful official or professional duties are excluded from the scope of the offence. Via a reference to the Code of Criminal Procedure (i.e. the Right to Refuse Testimony on Professional Grounds) in Subsection (3) No 2, this applies *inter alia* to "individuals who are or have been professionally involved in the preparation, production or dissemination of periodically printed matter, radio broadcasts, film documentaries or in the information and communication services involved in instruction or in the formation of opinion." This exemption is of particular interest for investigative journalists, because their research activities could constitute an offense under Subsection (1) in certain cases (e.g. if they acquire data from informers who committed a breach of official secrets). At the same time, Subsection (3) No 1 excludes certain acts of public officials from the offence. This exclusion has a declaratory rather than a substantive function.

Criticism

The introduction of Section 202d has been criticised for several reasons.[3]

1. The broad scope of the offence is problematic. In this respect, Section 202d could violate the principle of legal certainty in Criminal Law. According to this principle, it should be clearly possible to deduct from the wording of the law whether an action constitutes a criminal offence. This is not necessarily the case with respect to the unlawful acts that are eligible as an offence prior to Handling Stolen Data. Therefore, the specific criminal liability risks for electronic communication and business transactions following from Section 202d are hardly predictable.
2. The existence of regulatory gaps for the handling of stolen data is doubtful. The German Criminal Code, criminal offences under the Act Against Unfair Competition (Section 17) and the Federal Data Protection Act (Section 44) already provide a detailed Criminal Law framework for the unlawful handling of data. In particular, Section 44 of the Federal Data Protection Act provides a wide-ranging protection. Among other things, it criminalises the illegitimate collection and processing of personal data. Technically speaking, Section 44 also covers the conduct of data traders who act as middlemen on a "black market" for "stolen" data. The practical relevance of these existing provisions is, however, relatively low. Since 2007, not a single offender has been convicted to imprisonment under Section 44 Federal Data Protection Act according to the statistics of criminal convictions. There were never more than eleven perpetrators (sentenced to a fine) associated with Section 44 in a single year. This indicates that an insufficient enforcement – rather than a regulatory gap – is the true deficit of Criminal Data Protection Law.
3. The tendency to treat data similar to material goods in Criminal Law is flawed. Since data is potentially everywhere, it cannot be "stolen" in the same way as material goods. Handling stolen goods is a form of wrongdoing that consists in perpetuating the unlawful possession of a good that is no longer in possession of its rightful owner. This is clearly not the case if data is unlawfully copied because the data can still remain with its original "owner" and be "stolen" at the same time. This is why it is questionable if a "formal right of disposal" over data exists that is comparable to the right to ownership over material goods.
4. In the public debate, high attention has been paid to the possible infringement of the constitutional guarantees of free communication and expression following from the introduction of the new offence. In particular, the potential criminalisation of whistleblowers and (investigative) journalists has become a core topic. The disclosure of data gained by whistleblowers could indeed fulfil the elements of the offence of Handling Stolen Data, even though it would be necessary that the disclosure be performed with the intent of enriching the whistleblower, journalist or another, or of harming another. However, the constitutional protection of freedom of communication calls for a restrictive interpretation of Section 202d Criminal Code. In the light of this, according to Subsection 3, disclosures by whistleblowers would either be justified or excluded from the scope of the offence if there is a legitimate public interest in the concerned information.
5. Finally, the circumstances under which Section 202d was introduced have led to some criticism. Because the short amendment to the Criminal Code was introduced in one legislative act together with the introduction of the voluminous new rules on telecommunication data retention, it has been called a "submarine law".[4] It is likely that this context has constrained a more detailed debate about this new criminal offence with a potentially high impact on German Criminal Information Law.

AUTHOR

Dr Sebastian J. Golla is a postgraduate judicial service trainee at the Supreme Court of Berlin (Kammergericht), Germany.
Email: sebastian.golla@gmx.de

REFERENCES

1 Translation by the author.
2 Cf. in particular Deutscher Bundestag, Drucksache 18/5088, pp. 24 ff., 45 ff.
3 Cf. *Golla/von zur Mühlen*, Juristenzeitung 2014, pp. 668; Selz, in: Taeger, Internet der Dinge – Digitalisierung von Wirtschaft und Gesellschaft, Tagungsband DSRI-Herbstakademie 2015, 2015, pp. 915; *Beck/Meinicke*, Computer und Recht 2015, pp. 481.
4 http://heise.de/-2842118

Your money or your life? Modi's enactment of India's ID law

By **Graham Greenleaf**.

India's Modi government inherited from its Congress government predecessors a national ID system, the Aadhaar,[1] which has enrolled up to 800 million of India's 1.2 billion residents since 2009. Legislation to legitimise the system had been stalled in India's lower house (the Lok Sabha) since 2010, partly because of privacy concerns of legislators. Modi's government enthusiastically accepted this gift, promoting its expansion and defending it in the courts against constitutional claims that it infringed privacy.

However, the Supreme Court still presented a potential legal roadblock, with a case concerning the Aadhaar's constitutionality having been referred to a 'constitution bench' (to be appointed by the Chief Justice) for determination. Lack of a majority in the upper house (Rajya Sabha) presented a political obstacle to obtaining legislative legitimacy for the system, which still depended on a 2009 Executive decision for its imprimatur. This serial has had many episodes since 2009.[2]

This article explains how the Aadhaar legislation has unexpectedly been enacted, the basic structure of the ID system it establishes, its potential private sector uses, the privacy vacuum within which it will operate, and how it is now much more dangerous as a result of this enactment. A concluding question is whether this Bill is what Indians have been led to expect for the last seven years, or whether they have been deceived?

A Money Bill or maybe not

In what has been described as a "masterstroke"[3] – but one of dubious legality – the Modi government introduced the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill 2016 ('Aadhaar Bill')[4] into the Lok Sabha on 3 March 2016 as a 'Money Bill'. This characterisation (agreed to by a compliant Speaker) means that the Rajya Sabha cannot stop the passage of the bill and may only make suggestions concerning it. Nor do Money Bills have to go before Parliamentary committees. The Bill passed the Lok Sabha on 11 March and will be considered approved on 25 March, because the government will not accept recommendations suggested by the Rajya Sabha.[5]

Article 110(1) of India's Constitution provides that 'a Bill shall be deemed to be a Money Bill if it contains only provisions dealing with all or any of the following matters, namely', and there follows a list of six types of financial matters (a)-(f) (in short, taxes, government borrowings, custody or appropriation of consolidated funds, charges on them, and receipt of monies for them), plus '(g) any matter incidental to any of the matters specified in sub clause (a) to (f)'.

Few, if any, of the 59 clauses of the 2016 Bill deal directly with such 'money matters', with the exception of cl. 7 'Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc.' It would therefore seem questionable whether all remaining 58 clauses can be regarded as 'incidental' to cl. 7. Alternatively, perhaps the establishment of the world's most comprehensive biometric identification system, and the creation and regulation of the organisation which will run it, is in fact the substance of the Bill. The Aadhaar Bill is similar in many respects to the previous government's The National Identification Authority of India Bill 2010, which was not described as a 'Money Bill', but did not include an equivalent to cl. 7.

However, sub-article 10(3) of the Constitution says "If any question arises whether a Bill is a Money Bill or not, the decision of the Speaker of the House of the People thereon shall be final". The Speaker is reported to have taken a robust approach to this question: "First Speaker GV Mavalankar stressed that the word 'only' was not 'restrictive' and if a Bill dealt with a tax, it could also have provisions necessary for administration of that tax."[6]

The extent to which Article 110(1) can be satisfied by such fictions cannot be addressed here, but may become yet another constitutional issue before India's courts. The Congress Party, which also has a chequered history in abusing the Money Bills provision, has threated a court challenge.[7] In the meantime, the reality (even if temporary) of the soon-to-be Aadhaar Act must be addressed.

Mandatory use confirmed

Just as breathing is only mandatory if you wish to stay alive, obtaining an Aadhaar will only be mandatory for most people in India if they wish to avail themselves of government services (or many private sector services). Section 7 states that the Central Government or a State Government may "for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service" paid from central government funds "require that such individual undergo authentication, or furnish proof of possession of Aadhaar number". Where an applicant does not yet have an ID number, the government may require that "such individual makes an application for enrolment". In the interim "the individual shall be offered alternate and viable means of identification" that they can provide until their Aadhaar number is allocated. One of the amendments proposed by the Rajya Sabha, but rejected by the government, would have stated that an individual could choose "not to opt for enrolment" for an ID number, but instead provide "alternate and viable means of identification".[8]

Section 7 is the core mechanism by which the Aadhaar is made mandatory. Attempts to achieve this without legislative authority have led to the cases

now before the courts. There was no equivalent to this clause in the 2010 Bill (as discussed in the conclusion). Once governments can impose this mandatory requirement, pervasive use of the ID number follows rather easily. Governments and the private sector can accept the ID number "as proof of identity … for any purpose" (s4(3)), and the private sector can make its provision (but not its authentication) mandatory wherever it wishes.

Life-long surveillance

The Act establishes the Unique Identification Authority of India (UIDAI – the Authority) which "may engage one or more entities" to maintain the Central Identities Data Repository (CIDR) (s10) for which it is responsible.

The UIDAI "may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information" in the CIDR (s6). If addresses are required by regulations to be updated, perhaps this may be required every time a person has to have their identity authenticated, or perhaps on other events such as voting. Updating of photos may be periodically required. Since children will have ID numbers, CIDR data could accumulate over a person's whole life. There are no provisions for individuals to request that data be removed from the CIDR, and a proposed Rajya Sabha amendment to this effect was rejected by the government.

Time and circumstance, impossible to predict, will reveal to what extent CIDR data will be required to be updated. However, the CIDR has the potential to become a location register for India's people, a core form of surveillance in countries such as China and Vietnam, but one that has not occurred in modern India.

A further aspect of this continuous record of surveillance is that, although the CIDR will not record the reason for an authentication enquiry, it will record "the identity of the requesting entity" (s2(d)). The identity of some requesting entities may be very revealing, either from the public sector (e.g. police) or private sector (e.g. a clinic). The dangers of misuse are obvious.

Authentication, uses, and 'sharing'

Any government agency, or a business or person (corporate or individual) may be a "requesting entity" (s2(u)) entitled to obtain authentication from the authority of the "biometric information or demographic information" of an ID number holder (s8). The requesting entity must obtain the person's consent to collect this "identity information" for the purpose of authentication (according to regulations), and only use it to submit it to the Central Identities Data Repository (CIDR).

The CIDR can reply with a simple "yes" or "no" response, or with "any other appropriate response sharing such identity information, excluding any core biometric information" (i.e. fingerprints and iris scans). The CIDR may therefore provide a requesting entity with any demographic information it holds (e.g. address, age) and any other biometric information (i.e. photographs). Regulations will specify the circumstances under which the CIDR can share identity information with requesting entities (s29(2)). The 2010 Bill was fundamentally different, only allowing (in cl. 5(2)) "any other appropriate response excluding any demographic information and biometric information." This 2010 Bill did not allow CIDR to "share" addresses, age or photographs.

In the 2016 Bill, individuals must be told by the requesting entity what information may be "shared" after authentication, and to what uses they will put the information they receive. The requesting entity must tell individuals the uses to which it will put authenticated identity information, and obtain their consent before disclosing it further (s29(3)), or they will be subject to penalties. While they must be told "alternative of submission to identity information", if over 90% of Indian adults already have Aadhaar numbers (as the government claims), then alternatives will be illusory.

ID numbers, and "core biometrics" (fingerprints and iris scans) cannot be published or otherwise displayed, except if allowed by regulations (s29(4)). This implies that other authenticated ID information, including photos, can be so used (subject to notice to individuals).

Private sector implications

Despite its administration within the public sector, the Aadhaar will have profound long-term implications for the operation of all aspects of the private sector operating in India, whether in relation to their customers, their employees, or any other individuals with whom they deal. This purpose is stated clearly: "An Aadhaar number, in physical or electronic form … may be accepted as proof of identity … for any purpose" (s4(2)., and reiterated in both s57 and in s4(3) in differing words. There is no prohibition on private sector entities to make provision of an ID number mandatory for any transactions they wish.

It is clear from the above details that it is expected to be routine for any business in India that finds it useful to collect ID numbers, to obtain and/or authenticate further "identity information" from the CIDR, and make extensive uses, including disclosures, of that information. While the uses of identity information in any social setting are difficult to predict,[9] there is clearly no intention by the Indian government to keep much control over the private sector uses of this ID system. The ramifications of this deserve more detailed exploration.

Built-in disclosures – Court orders and national security

"Core biometric information" (fingerprints, iris scans, and any other biometrics specified by regulations) cannot be "shared with anyone for any reason whatsoever" or used (including by CIDR) other than for authentication or to generate ID numbers (s29(1)). This information is therefore exempt from the following disclosures, but can be used to authenticate supposed identities (e.g. against a fingerprint provided by a court or a security agency).

Any court (District Court or above) may order the CIDR, or any "requesting entity" (public or private sector bodies) to disclose any identity information (e.g. addresses and photographs) it holds (s33(1)). There are no limitations imposed, so this could apply to orders in both criminal and civil matters, and may apply to judicial warrants.

Any specially authorised official

"not below the rank of Joint Secretary" may issue directions "in the interest of national security", for disclosures by the CIDR, or any "requesting entity", of any identity information or "authentication records" (s33(2)). Any such direction must be reviewed "before it takes effect" by an Oversight Committee.

Privacy law vacuum continues

Other than the minimal limits on use of Aadhaar information referred to above, India has no significant privacy protections:

- Although biometric information collected under the Aadhaar Act is deemed by s30 to be "sensitive personal data or information" for the purposes of s43A of the Information Technology Act 2000 (under which India's rudimentary data privacy "Rules" were made), this will be of little benefit. Section 30 will not prevent government abuses, because s43A and the Rules only apply to companies or bodies "engaged in commercial or professional activities". While the UIDAI is created as a "body corporate", it is not a company, and it is engaged in public administration, not commerce or a profession. Where private companies collect biometrics in the course of ID creation or authentication, s30 may have some application but the whole system of s43A protections is flawed.[10]
- The Aadhaar Act does not in itself include any set of data privacy provisions, beyond a few basics of access and correction rights, protection of CIDR security, and the integrity of the enrolment/authentication processes. It does not provide remedies for individuals, and only the Authority can initiate any of its penal provisions (s47(1)).
- No comprehensive data privacy legislation has been enacted in India, though it has been proposed on numerous occasions at high levels of government.[11]
- The Modi government is arguing in the ongoing Puttaswamy Case that India's constitution does not provide any protection for privacy (despite long-held assumptions that case-law showed otherwise).[12]

India's lack of privacy protections will now be much more dangerous with the enactment of the Aadhaar Act. The CIDR is dangerous in itself. Records in both public sector and private sector systems will become more consistent because of Aadhaar authentication, and data matching between them will therefore be facilitated, while remaining unregulated.

Conclusion: Function creep by legislative deception

Seven years ago the Aadhaar (or UID as it was then called) was introduced as a voluntary ID number, and governments and the UIDAI constantly stressed that was so, even though this was difficult to believe.[13] The 2010 Bill did not make use of the number mandatory for any government services. Throughout the challenges in the Supreme Court to government attempts to make the use of the ID number mandatory during 2014-15, governments continued to insist that its use was voluntary. Now, after almost all of India's population has obtained an Aadhaar, the 2016 legislation includes s7 which allows governments to make its use mandatory for key government benefits. In addition, while the 2010 Bill did not allow the CIDR to share address, age or photograph data, the 2016 legislation does allow this.

There are also many loopholes in the Bill where expansion by regulations is allowed,[14] and the regulations are made by the Authority itself. These include the definitions of the data that is the essence of the system ("biometric data", "core biometric data" and "demographic data"), and the requirements to update the CIDR, not only administrative matters concerning registration and authentication. The Aadhaar system is therefore unstable and deceptive at its core.

ID systems are prone to "function creep", the incremental expansion of their functions, often contrary to promises made by politicians when the systems are introduced. There are few examples as blatant, even though they were predicted, as the Aadhaar's final admission of legislative compulsion, and its conversion of the CIDR from a uni-directional to a bi-directional flow of information. Much more needs to be said about the Aadhaar Act, but these are its essential deceptions.

INFORMATION

Thanks to Elonnai Hickock for providing very valuable comments on a draft. Responsibility for all content remains with the author.

REFERENCES

1 Aadhaar means 'foundation' or 'base'.
2 For background, see articles cited herein.
3 Gyanant Singh 'Aadhaar card is about privacy, not money' Businesstoday.in, 16 March, 2016 www.businesstoday.in/current/policy/aadhaar-card-is-about-privacy-not-money/story/230292.html
4 Aadhaar Bill as passed by Lok Sabha 11 March 2016 www.prsindia.org/uploads/media/AADHAAR/Aadhaar%20bill%20as%20passed%20by%20LS.pdf
5 The Wire Staff 'Three Rajya Sabha Amendments That Will Shape the Aadhaar Debate' *The Wire* 16 March 2016 http://thewire.in/2016/03/16/three-rajya-sabha-amendments-that-will-shape-the-aadhaar-debate-24993/
6 Gayant Singh, above.
7 Times of India (staff report) 'Aadhaar Bill: All you need to know' *Times of India* 17 March 2016; The government refers to 'the juvenile justice bill and the workman injury compensation bill that the Congress brought as money bills when it was in power.'
8 *The Wire*, above cited.
9 'U Rao and G Greenleaf 'Subverting ID from Above and Below: The Uncertain Shaping of India's New Instrument of E-Governance' *Surveillance & Society* (2013) http://ssrn.com/abstract=2350631
10 G Greenleaf 'India's Data Protection Impasse: Conflict at All Levels, Privacy Absent' *Privacy Laws & Business International Report*, February 2014, pp 23-24.
11 G Greenleaf 'India's Draft the Right to Privacy Bill 2014 – Will Modi's BJP Enact it?' *Privacy Laws & Business International Report*, June 2014, pp. 21-24.
12 G Greenleaf 'Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number' Privacy Laws & Business International Report, Oct 2015, pp.24-26.
13 G Greenleaf 'India's National ID System: Danger Grows in a Privacy Vacuum' *Computer Law & Security Review*, Vol. 26, No. 5, pp. 479-491, 2010.
14 See in particular s2(g), s2(j), s2(k), s2(m), s4(3), s5, s6, s8, s10, s23 (various ss.), s28(5), s29(4), s31, s32, s54 and s55.

The limits of the US Judicial Redress Act

Edward Hasbrouck analyses the new law which provides limited privacy rights for Europeans – and only for personal data processed by the US federal government.

European Union Commissioner for Justice, Věra Jourová, described the US Judicial Redress Act[1] signed into law by President Obama on 24 February 2016 as, "a historic achievement [that] will ensure that all EU citizens have the right to enforce data protection rights in US courts…. The entry into force of the Judicial Redress Act will pave the way for the signature of the EU-US Data Protection Umbrella Agreement."

But the limitations and exceptions in the Judicial Redress Act, and the experience of US citizens who have sought redress in US courts for privacy violations, cast doubt on whether this law will really "ensure that all EU citizens have the right to enforce data protection rights in US courts." There are likely to be few real-world cases in which the Judicial Redress Act will provide enforceable legal rights to citizens or residents of the EU, or anywhere else.

The Judicial Redress Act gives some foreign citizens some of the rights that US citizens currently have, with respect to some of the uses and misuses by the US government of their personal information. But in no case will any foreigner have more rights under the Judicial Redress Act than US citizens have under the Privacy Act[2].

Serious scrutiny of the terms of the Privacy Act, and of the history of attempts by US citizens to use the Privacy Act to protect ourselves against misuse of our personal information by the US government, has been largely absent from the debate about the Judicial Redress Act. But from our experience as the plaintiff in one of the key test cases in which US citizens have attempted to assert Privacy Act claims against the US government[3], we have learned an important lesson that Europeans need to know: the Privacy Act is so limited and riddled with exceptions that it is almost worthless.

All of the limitations and exceptions that always rendered the "protection" of the Privacy Act inadequate — even for US citizens — will continue to render the protection of the Judicial Redress Act inadequate for foreigners, in all of the same ways, and in additional ones.[4]

What are these exceptions and limitations? In order to make sense out of the Judicial Redress Act, it's essential to understand the exemptions in the Privacy Act, as courts have interpreted them.[5]

Federal agencies can exempt themselves from almost all of the requirements of the Privacy Act with respect to "investigatory material compiled for law enforcement purposes," a catch-all category that has been applied to records of dragnet surveillance and other information compiled and used for "pre-crime" profiling, even when the data subjects have never been accused or suspected of any crime. All an agency has to do to opt-out is to publish a notice in the Federal Register that a particular system of records has been declared exempt by the agency that maintains the records. An agency can wait to promulgate such a notice until after it receives a request for access to records, a request for an accounting of disclosures, or a request for correction of records.

Under the interpretation of the Privacy Act adopted by the US government and upheld by a Federal District Court – the court when it was challenged for the first time in our litigation, additional Privacy Act exemptions can be promulgated at any time in the future, and applied even to requests that had already been made. In light of this ruling, nobody can rely on any "rights" under the Privacy Act that could be retroactively revoked at any time. Once such exemptions are promulgated, individuals – even US citizens – have no right under US law to see what records are being kept about them, and no right to know how or according to what algorithms data about themselves is mined, processed, or otherwise used. No logs need be kept of who accesses records, or to whom they are disclosed.

The rules published by the US Department of Homeland Security to exempt records in the DHS Automated Targeting System (including commercial data about customers and other individuals obtained from private companies) from the requirements of the Privacy Act are typical of the exemptions that have been promulgated for numerous other systems of Federal records about individuals:

The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2).[6]

To understand what an exemption rule like this this means, one has to read the clauses of the Privacy Act referred to in the exemption rules. These DHS records have been exempted by the DHS from each of the following requirements of the Privacy Act:

- The right of a data subject to access records about herself.
- The right of a data subject to receive, on request, an accounting of disclosures of her personal data to other agencies or third parties.
- The prohibition on maintaining records about individuals that are not relevant and necessary to accomplish a legal purpose of the agency.
- The requirement to maintain records which are used in making determinations about individuals "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual."
- The requirement to collect personal information "to the greatest extent

practicable" directly from the data subject rather than from third parties.
- The requirement to notify data subjects of what information about them is being collected, and from whom it is being collected.
- The right of a data subject to to dispute, amend, or correct records about herself.
- The right of a data subject to add a notice of disputed data in records about herself, and to have that notice included whenever the disputed portion of the record is disclosed to a third party.

It's not just the DHS that has opted out of the Privacy Act. The NSA has similarly exempted its surveillance records from the Privacy Act: "The problem is that Europeans are likely to notice that the Privacy Act provides no meaningful redress to targets of NSA surveillance. Agencies can exempt themselves from the Privacy Act's access and redress provisions on grounds of national security. U.S.C. § 552a(k). The NSA has taken full advantage of this section. 32 C.F.R. § 322.7(a)."[7]

Once an agency has published a notice exempting a system of records from these requirements of the Privacy Act, it is completely legal (or at least, it is not a violation of the Privacy Act for which a US citizen or anyone else can sue the agency) for the agency to fill that database with secret information about individuals, collected from undisclosed third parties, that it knows is likely to be inaccurate, outdated, incomplete, and irrelevant to any lawful purpose. The agency can withhold all of this information from the data subject, and secretly disclose any or all of it to any other government agency or third party anywhere in the world. Any disclosure of exempt records that an agency chooses to make is "discretionary" and not subject to judicial review.

For the reasons discussed above, the Privacy Act gives US citizens inadequate legal protection. But even with the Judicial Redress Act, Europeans and other foreigners (even citizens of the most preferred foreign nations) will continue to have even less protection and fewer rights than US citizens, in at least two important ways that have not been widely noted.

First, even with respect to records that have not been exempted from the Privacy Act, the Judicial Redress Act gives foreign citizens the right to sue to enforce only some, but not all, of the rights that US citizens can sue to enforce under the Privacy Act. Specifically, foreign citizens can bring lawsuits in US courts only for violations of "section 552a(g)(1)(D) of title 5, United States Code" or "subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code" but not under any of the other provisions of the Privacy Act. These sections cover refusal by a Federal agency to comply with a subject access request or request for amendment of a record, but notably exclude lawsuits by foreigners for violations of subparagraph (C), which allows a US citizen to sue an agency that "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relation to … the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."

The exclusion of subparagraph (C) from the causes of action allowed by the Judicial Redress Act, while including subparagraphs (A), (B), and (D), appears deliberately crafted to preclude challenges by foreigners to the use of unreliable and irrelevant third-party data in profiling, risk assessments, and similar algorithmic processing and scoring systems.

Second, records are "covered" by the Judicial Redress Act only if they have been transferred:

(a) by a public authority of, or private entity within, a … covered country; and
(b) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.

This excludes two key categories of records: records maintained for

'SAFE HARBOR' REPLACEMENT : EUROPEANS' COMPLAINTS WILL TAKE PRIORITY OVER AMERICANS'

European and US negotiators have reached agreement on a plan for transfer of personal information across the Atlantic that continues to provide more protection by US agencies to Europeans than Americans.

Because of a decision by the European Court of Justice last October that invalidated the "Safe Harbor" scheme developed by the US Department of Commerce, a new agreement was necessary to continue permission for international companies to remove personal data from Europe

The European Commission on Feb. 2 announced agreement on a new "EU-US Privacy Shield," with only a few details:

• The US will establish an ombudsman in the Department of State to address complaints related to US intelligence authorities' access to data about Europeans. American citizens and residents have no such redress.

• The US Office of National Intelligence has made binding commitments that US access to Europeans' data for national security purposes will have "clear limitations, safeguards and oversight mechanisms" limiting the access to what is "necessary and proportionate." The US has also agreed to an annual review of these commitments. American citizens have no such assurances.

• The US Department of Commerce will monitor companies to ensure that they publish their privacy commitments, which then become enforceable by the Federal Trade Commission, similar to the previous Safe Harbor Framework. But the privacy policies need not provide any protections for Americans.

• European Union individuals will have access to free alternative dispute resolution mechanisms. Americans will not benefit from this.

• European regulators will have a formal channel to refer complaints to the US Department of Commerce and the FTC. Complaints from Europe will need to be resolved by stated deadlines, meaning that they will have priority over complaints by Americans, where there are no required deadlines.

• American companies participating in the new EU-US Privacy Shield will need to commit to "robust" obligations, including submission to European jurisdiction when transferring employee data.

In exchange the Europeans will issue an "adequacy decision' by this spring asserting that US privacy protections are "adequate" for transferring data from Europe to here. Presumably the agreement binds only the Obama Administration, not its successors.

By Robert Ellis Smith.

Reproduced with permission from Privacy Journal, February 2016 p.3 www.privacyjournal.net/

purposes other than enforcement of criminal laws, and records transferred from the EU to the US government by way of commercial intermediaries in the US (or in third countries that are not covered by the Judicial Redress Act).

Many US laws and regulations are enforced by civil, rather than criminal, sanctions. Records maintained by the US government for civil enforcement purposes are completely exempt from the Judicial Redress Act, as are all records maintained for any purpose except criminal law enforcement.

Records maintained for criminal law enforcement purposes can be (and almost always have been) exempted from the Privacy Act. Records maintained for any other purpose are exempt from the Judicial Redress Act. The result is that hardly any records will fall through the cracks between the exemptions in these two laws, and provide a basis for a lawsuit by a foreign citizen.

Even if either or both the Privacy Act and/or the Judicial Redress Act were amended to remove these exemptions, the limitation of the Judicial Redress Act to records transferred directly from an entity in the EU to the US government would leave a huge loophole, of exactly the sort the US has exploited in the past to intercept personal and commercial information about financial transfers between European banks from servers of SWIFT in the US, information about electronic communications between other countries from intermediaries in the US through which messages were routed, and airline reservation data ("passenger name records") collected by European airlines, travel agents, and tour operators stored with computerized reservation systems in the US.

The Privacy Act provides inadequate data protection for US citizens, and the Judicial Redress Act would provide even more inadequate protection for non-US citizens. Neither of these laws provides any basis for a finding that anyone's rights are adequately protected in the US, or for approval of the proposed "Privacy Shield" or the proposed EU-US "umbrella agreement" on data transfers.

AUTHOR

Edward Hasbrouck is consultant to the Identity Project – PapersPlease.org.
Email: edward@hasbrouck.org

REFERENCES

1 H.R. 1428, Judicial Redress Act of 2015, www.congress.gov/bill/114th-congress/house-bill/1428
2 5 U.S.C. § 552a
3 *Hasbrouck v. US Customs and Border Protection*, Case C 10-03793 RS, US District Court, Northern District of California. See case documents and discussion at https://papersplease.org/wp/hasbrouck-v-cbp/
4 See Robert Gelmann, 'Foreigners' privacy rights in the US: Little more than a gesture,' *PL&B International*, October 2014.
5 See the round-up of case law on Privacy Act exemptions compiled by the US Department of Justice at www.justice.gov/opcl/ten-exemptions
6 'Privacy Act of 1974: Implementation of Exemptions,' 75 Federal Register 5487-5491, 3 February 2010, www.gpo.gov/fdsys/pkg/FR-2010-02-03/html/2010-2201.htm
7 Timothy Edgar, 'Redress for NSA Surveillance: The Devil Is in the Details', Lawfare blog, 19 October 2015, www.lawfareblog.com/redress-nsa-surveillance-devil-details

Belgian DPA vs Facebook update

Stewart Dresner visited Willem Debeuckelaere, Belgium's DPA, at his Brussels office.

The case of Belgium's Data Protection Commission against Facebook was reported (*PL&B International* December 2015 p.1) but questions remain.

PL&B: Has Facebook paid your penalty of €250,000 per day?
Debeuckelaere: Belgium's Commission does not have the power to impose a fine so cannot enforce its order but a court can enforce a financial sanction. Facebook appealed objecting to my order (*dwangsom* in Flemish and *astreinte* in French). The Court of First Instance in Brussels in its decision of 9 November 2015 confirmed that this case is within its jurisdiction, as Facebook has an office in Belgium and that this amount was proportionate in relation to the company's revenues and profits worldwide. The Court took the decision that Facebook must pay this amount if it does not comply with the DPA's written order.[1] However, Facebook did comply with the order within the required time frame of 48 hours. It did so by preventing Facebook non-account holders in Belgium from accessing open information on its network, basing its implementation on Belgian Internet Protocol addresses.

PL&B: What will happen next?
Debeuckelaere: Facebook has appealed to the Court of Appeal and the case is due to be heard starting on 1 June 2016, and a decision is expected within one month.

PL&B: Is anything else happening in the meantime regarding this case?
Debeuckelaere: Yes, my team have held face-to-face meetings in my office with Facebook's EU-based and US-based managers without lawyers present. We have announced publicly that we have held these meetings but we are not revealing the content of the discussions.

PL&B: What is happening with the Facebook DPA contact group which issued its Common Statement on 4 December 2015.[2] stating that Facebook should follow the Belgian DPA's order to Facebook on consent across all the EU Member States?
Debeuckelaere: Although we in Belgium acted first, the Netherlands DPA is the leader of this group. They

are conducting an administrative procedure/investigation but as confidentiality is written into their law, they have made no announcement and even we, the neighbouring DPA in Belgium, do not know how they are progressing.

France's CNIL announced in February that it had given Facebook three months to fix consent or face sanctions.[3]

Spain's DPA, the AEPD, is conducting its own investigation and may wait without taking action until these cases against Facebook are discussed in the Art. 29 DP Working Party, currently scheduled for its June meeting.

In addition to exchange of information within the Contact Group by electronic communications, there have also been coordination meetings in Hamburg, The Hague and Madrid.

Legal action has been taken by Germany's state (Land) DPAs in Hamburg and Schleswig-Holstein.[4] However, a German judge has declared that his court is not competent to deal with this case and that it should be referred to the Court of Justice of the EU.

I agree that the European Court should set the lines of a global settlement of the Facebook case with a common enforcement programme. 90% of Belgian law is the same as EU law so a Belgian judge would normally follow the lead of the European Court.

PL&B: Do you have any other news?
Debeuckelaere: Yesterday, (7 March), I signed an approval of the Binding Corporate Rules (BCR) application by US pharmaceutical company, Merck Sharpe & Dhome. The Belgian Commission, the lead authority, completed its review within two and a half months but the total approval time with the two other DPAs assisting the process, was one year and three months. But I do not criticize the other DPAs, as everyone has their resource constraints. Here in the Belgian DPA, we also have our language constraints. Our staff are civil servants with no requirement to be bilingual. However, I have taken a decision, which needs to be approved by the legislature, that all new staff should be bilingual. Bilingual can mean, for example, Flemish-French, French-English, or Flemish-English. So this decision will not automatically result in more staff who can work in English, which is the language of BCR applications and approvals.

PL&B: What is your view of the secretariat of the new European Data Protection Board being provided by the European Data Protection Supervisor?
Debeuckelaere: I am happy with this decision because the EDPS: has a tradition of high quality work; employs staff from many EU Member States so has diverse perspectives and language skills; has experience in many fields; and has staff with many personal links with national DPAs.

The current President of the EU Art. 29 DP Working Party, Isabelle Falque-Pierrotin, President of France's CNIL, had her mandate renewed in February this year. But it is very difficult to be head of a national DPA and be President of the new European Data Protection Board, both in terms of chairing meetings in an impartial way and having a double workload. Therefore, I am in favour of the President of the new European Data Protection Board being a full-time job.

INFORMATION

Willem Debeuckelaere, President, Belgium's Commission for the Protection of Privacy, will speak at *Great Expectations*, *PL&B's* 29th Annual International Conference, 4-6 July 2016 at St. Johns' College, Cambridge.

REFERENCES

1 The Tribunal's judgement in English: https://www.privacycommission.be/sites/privacycommission/files/documents/Judgement%20Belgian%20Privacy%20Commission%20v.%2Facebook%20-%2009-11-2015.pdf
Other source material is shown in *PL&B International* December 2015 p.29
2 www.privacycommission.be/en/search/site/Common%20Statement%20by%20the%20Contact%20Group%20of%20the%20Data%20Protection%20Authorities
3 www.privacylaws.com/Publications/enews/International-E-news/Dates/2016/2/CNIL-gives-Facebook-3-months-to-fix-consent-or-face-sanctions/
4 www.privacylaws.com/Publications/enews/International-E-news/Dates/2016/1/Facebook-v-Belgian-DPA-case-to-go-to-appeal-and-a-German-case-moves-up-to-the-Federal-Court/

Impact of the European Data Protection Board

The EU Data Protection Authorities have published their Article 29 DP Working Party programme. It highlights the level of cooperation needed and the importance of the European Data Protection Board (EDPB) which will replace the Article 29 DP Working Party under the EU Data Protection General Regulation (GDPR) when it enters into force. The DPAs are to set up an EDPB task force to ensure that the Board will be ready to function from day one of the new regime. The secretariat will be provided by the EU Data Protection Supervisor (EDPS) "under the instructions" of the Chair of the EDPB. The secretariat will have an important role in administering the One-Stop-Shop and the consistency mechanism. These developments are also important for companies when they need to designate a lead Data Protection Authority to resolve data protection issues involving more than one EU Member State.

The Board will issue guidance for controllers and processors – for example, on the data portability right (p.7), Data Protection Impact Assessments (*PL&B UK Report* March 2016 pp.15-17), certifications, and the role of DPOs (*PL&B UK* March 2016, pp. 7-9).

The DPAs say that their action plan will be reviewed periodically and the Article 29 DP Working Party will regularly consult business representatives and civil society representatives on their views regarding implementation of the GPDR.

• *The DPAs' 2 February statement: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf*

GDPR's extra-territoriality means trouble for cloud computing

Extending the reach of the EU Data Protection Regulation may motivate non-EU controllers to avoid using EU processors. By **Kuan Hon**.

The proposed General Data Protection Regulation (GDPR) would widen the territorial scope of EU data protection laws.[1] The Council of Ministers' draft statement of reasons on its position at first reading[2] gives the flavour: "creates a level playing field for controllers and processors in terms of territorial scope by covering all controllers and processors irrespective whether they are established in the Union or not".

The "equipment" ground of applicability, under the current Data Protection Directive (DP Directive), would be replaced by a new ground based on "offering" goods or services to EU data subjects or "monitoring" their behaviour occurring in the EU. When coupled with the GDPR's new direct regulation of processors, not just controllers, the implications of this extra-territorial expansion of EU data protection laws could be far-reaching and, in cases such as cloud computing, even absurd and unfair, with possible negative consequences as I will discuss.

Comparative table

The table below compares relevant provisions of the DP Directive and GDPR.[3] As can be seen, the "international law" ground – intended for Member State embassies in foreign countries – would be unchanged, and I won't cover it further here.

Establishment

GDPR repeats the DP Directive's phrase, "context of activities of an establishment". This means the CJEU's[4] very broad interpretation of the "establishment" ground under *Google Spain*[5] will probably continue to apply. The GDPR would explicitly confirm EU data protection laws' applicability to worldwide personal data processing under this ground ("regardless of whether the processing takes place in the Union or not"), generally considered to be the case anyway. Most significantly, the "establishment" ground would extend to processors - but the unclear drafting creates legal uncertainty.

COMPARISON OF THE EU DP DIRECTIVE, GDPR AND INTERNATIONAL LAW

	DP Directive Member States must apply national data protection laws to processing of personal data where:	GDPR applies to
Establishment	Art. 3(1)(a) …the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;	Art. 3(1) …the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
Equipment to "offering"/ "monitoring"	Art. 3(1)(c) …the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community	Art. 3(2) …the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union
International law	Art. 3(1)(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law	Art. 3(3) …the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law

Suppose a non-EU-established controller, say a US corporation, with no other connections to the EU, uses an EU-incorporated processor to process personal data of the corporation's US customers. This processing would be in the context of the activities of the EU-established processor, so the GDPR would apply no matter where the processor physically processes the data (recall that "processing" includes mere storage or transmission). However, would this mean that only GDPR's processor obligations apply to the EU processor, such as obligations regarding security (Art. 30) and record-keeping (Art. 28)? Or would GDPR's controller obligations also apply to the non-EU controller, because it chose to use an EU-established processor? I hope not, but this can't be ruled out as a possible risk for the controller, given the CJEU's inclination to interpret data protection law provisions broadly. While the new "offering" ground would only apply to processing of personal data of data subjects in the EU, the "establishment" ground's applicability is not qualified by reference to location or citizenship of the data subjects concerned. If using an EU processor would subject a US controller to GDPR in its entirety, even where the processing relates only to US data subjects' personal data, might this motivate US (indeed other non-EU) controllers to avoid using the services of EU processors, and/or motivate processors not to establish in the EU or to close or reduce EU operations?

Even assuming that the GDPR would apply only to the EU processor, GDPR's requirements on processors may affect their controllers. Notably, processor contracts must be governed by EU or Member State law, and contain certain minimum terms (Art. 26) – and these requirements are not imposed only on controllers; the wording appears to apply equally to controllers and processors. Art. 26 would restrict parties' freedom to contract on their own terms.[6] To avoid possible fines of €10 million (or 2% of total worldwide annual turnover if greater) under Art. 79(3)(a), processors must contract on Art. 26 terms. But, while Art. 26's mandatory contract terms were intended to protect controllers, in fact non-EU controllers may not wish to incorporate them. For example, a US controller may want the law of California or another US state to apply to its processor contracts. As another illustration, when controllers use infrastructure cloud services (IaaS, PaaS, storage SaaS) to process personal data, they process the data themselves in self-service fashion, using providers' technology infrastructure. Generally, those providers monitor controllers' usage only for billing/support purposes. Such controllers may not wish to tell providers the subject-matter/duration of their processing, the processing's nature/purpose, type of personal data processed or categories of data subjects – nor would providers wish to know that information. However, under Art. 26, controllers and processors have no choice – the contract must contain that information. Hence, again, non-EU controllers may be motivated to avoid using EU processors.

Equipment and offering/monitoring

The DP Directive's "equipment" ground has been problematic. Storing or reading cookies on or from EU data subjects' computers or mobiles involves "equipment" use, with EU regulators, the Article 29 Working Party, acknowledging the unsatisfactory consequences "that European data protection law is applicable in cases where there is a limited connection with the EU".[7] Abolishing the "equipment" ground would stop EU data protection laws from applying to non-EU controllers who merely use EU data centres to process personal data. However, the "establishment" and "offering" grounds could still catch such controllers. For example, an EU data centre, if dedicated to the use of the non-EU controller, might be considered its "establishment", even if owned/run by a third party.[8]

The replacement "offering/monitoring" ground focuses much more clearly and directly on the core underlying policy objective of protecting EU residents targeted by non-EU entities. However, it's not without its issues. Instead of using the recognised EU concept of "targeting", GDPR refers to "offering", whose meaning is much less settled. It's broader than "targeting" – "envisaging" the offering of goods/services to EU data subjects seems enough, such as mentioning EU customers/users (Rec. 20).

What's more troubling is the inclusion of processors under this ground in an expansive, insufficiently-circumscribed way. To illustrate, suppose a US corporation creates an e-commerce website for selling goods/services to its customers, including EU residents, using a third party US hosting provider's service (cloud-based or otherwise). Customer data is stored on the website's backend database, on the provider's infrastructure. Et voila, the provider is a "processor"! The processing is "related to" the US corporation's offering of goods/services to EU data subjects, so the provider is caught by GDPR, including potential liability for compensation[9] – even if it may have no connection with the EU, other than its service/infrastructure being used by a controller to provide goods/services (including free services) to EU and other customers.

Now, there are good and fair policy reasons why the GDPR should attempt to catch the US controller. However, applying GDPR to non-EU providers of technology infrastructure goes too far, in my view. Nonetheless, it is what it is.

"Monitoring" involves, not watching someone live, but rather "whether individuals are tracked on the Internet including potential subsequent use of data processing techniques which consist of profiling an

> Applying GDPR to non-EU providers of technology infrastructure goes too far.

individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes" (Rec. 21). This means that subsequent analysis of EU residents' personal data, "including" profiling, could bring the analysing non-EU controller within GDPR's net – and even non-EU processors whose services are used for the analysis, like cloud providers. This makes it more important that such data are anonymised before analysis, if compatible with the use case contemplated.

Where the offering/monitoring ground applies, "the controller or the processor" must, on pain of a fine of €10 million or 2% total worldwide turnover if higher (Art. 77(3)(a)), designate in writing an EU representative to deal with regulators/data subjects, ensure compliance with GDPR (Art. 25), and suffer enforcement action for "controller" non-compliance (Rec. 63). No representative is required where the processing is by a public authority/body, or where processing is "occasional", does not include "on a large scale" processing of special categories of data[10] or criminal convictions/offences data, and "is unlikely" to result in "a risk" for individuals. As any processing of personal data could pose "a risk", in practice it seems only non-EU public authorities can escape having to appoint representatives.

Is Art. 25 satisfied if only the controller designates a representative, but the processor whose technology infrastructure is used by the controller does not, because only one of them needs to ("or")? Or is the word "or" intended to mean either or both controller and processor, whoever the offering ground applies to? This uncertainty is unhelpful.

Because it's difficult to enforce EU data protection laws outside the EU (discussed further below), it's unsurprising that DP Directive's Art. 4(2)'s similar requirement, for non-EU controllers caught by the "equipment" ground to appoint EU representatives, has been largely ignored. However, the prospect of big fines under GDPR for non-appointment may force non-EU controllers and processors, at least if they have any EU assets or other EU presence, to grapple with GDPR Arts. 3 and 25.

Enforcement?

The elephant in the room is GDPR's extra-territorial enforceability. How can EU regulators compel non-EU controllers or processors to pay fines, take required actions etc? Despite long-standing efforts by the Hague Conference,[11] resulting in proposed text for a suitable Convention,[12] no international agreement seems in sight on cross-border recognition and enforcement of judgments – still less of administrative fines such as those to be levied under GDPR. EU regulators have already acknowledged the unsatisfactory consequences of using the "equipment" ground to apply EU data protection laws in situations with limited EU connection. In such situations, particularly where the connection to the processing itself and a processor's true control over privacy risks is also limited (as where a processor's technology infrastructure is used by a non-EU controller, but the processor does not actively process personal data for the controller), non-EU courts/authorities may be reluctant to enforce GDPR fines against non-EU processors, as they might (with some justification) consider that GDPR's extra-territoriality over-reaches.[13]

However, for caution's sake, and in view of large potential fines as well as reputational impact, some non-EU controllers/processors might still strive to comply with GDPR even if it is unlikely to be enforceable against them in practice. Certainly, those with some EU presence may feel under more pressure to do so.

Practical implications

For EU-"established" controllers, their worldwide personal data processing will remain within scope, although *Google Spain* has broadened the "establishment" ground's territorial reach considerably.

GDPR's regulation would be tougher and more prescriptive, while not necessarily achieving technology-neutrality,[14] with possible competition/anti-trust-scale fines for breach. Therefore, controllers with no other EU connection might avoid building or using EU data centres, at least where a data centre could be treated as the controller's "establishment". Such non-EU controllers may also be deterred from engaging EU processors to process their personal data, particularly data of non-EU residents, because of the risk that the GDPR could thereby apply to such controllers, although in practice controllers are also likely to consider risks of practical enforcement and the size of potential fines. So, to avoid losing business from non-EU controllers, some EU processors might set up non-EU processing affiliates, which could even process personal data in EU data centres post-GDPR – if their processing is not considered "in the context of" activities of the EU processor (a big "if"!). Structural changes to corporate groups and business segregation may result (perhaps even moving corporate HQs/parent companies outside the EU?), and costs will probably be passed to end users ultimately.

EU-"established" processors, again bearing in mind the wide interpretation of "established", must obviously comply with GDPR as regards their worldwide personal data processing. Because GDPR may apply to non-EU-established processors whose technology infrastructure are merely used by others to offer goods/services to EU residents or "monitor" their behaviour, such processors could decline to service non-EU customers who intend to offer goods/services to EU residents or monitor them, insisting on appropriate warranties/indemnities to that effect (or that such customers must appoint EU representatives if EU residents' personal data could be involved, with indemnities). Again, the practical likelihood of enforcement, size of fines and reputational issues will probably factor into the risk equation. With limited resources, regulators will probably focus their enforcement efforts strategically, and some organisations are more likely than others to be targeted.

Generally, anonymisation of personal data may be incentivised, although that can be tricky to achieve properly in practice, and is not possible for some intended uses.

Policy issues

GDPR's provisions on territorial scope, together with *Google Spain* and GDPR's tighter restrictions on international transfers of personal data and "onward transfers",[15] mean that effectively the EU is exporting its data protection laws to the world, and compelling compliance with EU data protection standards worldwide. Would other countries accept this, or might they consider it an intrusion too far into their sovereignty, particularly in cases where the EU connection is low and their local processors' control of personal data is minimal? Also, from an EU perspective, in the worst case scenario, could GDPR trigger a flight of businesses (and loss of jobs and reduced availability of services, free or paid) from the EU?

Guidance on the uncertainties regarding GDPR's territorial scope is sorely needed. It is not envisaged by the Art. 29 Working Party's current GDPR action plan,[16] but hopefully they will address it in 2017?

AUTHOR

Dr Kuan Hon is a consultant lawyer for Pinsent Masons and senior researcher with QMUL, but this article is written purely in her personal capacity and should not be taken to represent the views of any organisation with whom she may be associated.
www.kuan0.com

REFERENCES

1 This article discusses only the GDPR's extra-EU applicability, not issues with the so-called "One Stop Shop" within the EU. Those merit separate consideration, particularly which EU Member State's laws apply to a processing, and which national regulator(s) may have jurisdiction when a controller or processor has businesses or operations in multiple Member States.
2 http://data.consilium.europa.eu/doc/document/ST-5419-2016-ADD-1/en/pdf
3 References herein are to the politically-agreed version at http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf. GDPR may be formally adopted "around July" 2016, taking effect 2 years later https://iconewsblog.wordpress.com/2016/03/14/a-data-dozen-to-prepare-for-reform/.
4 Court of Justice of the European Union.
5 ECLI:EU:C:2014:317 http://curia.europa.eu/juris/liste.jsf?num=C-131/12. This held that "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of [Art. 4(1)(a) DPD], when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State". Thus the DP Directive applied directly to the (non-EU) search engine operator, not just to its Member State subsidiary, effectively piercing the "corporate veil". Therefore, establishing an EU subsidiary may subject non-EU entities to EU data protection laws if the subsidiary's activities are "inextricably linked" to its parent's activities, but not if they are not - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf.
6 On problems that Art. 26 would pose for service providers, and for cloud use, see www.scl.org/site.aspx?i=ed43376 and www.scl.org/site.aspx?i=ed46375.
7 WP179 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf p.21; updated (not on this point) by http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf.
8 See Hon, Millard & Hörnle, "Which Law(s) Apply to Personal Data in Clouds?", Chapter 9, Cloud Computing Law (Millard (ed), OUP 2013) and http://ssrn.com/abstract=2405971.
9 See fn. 6.
10 Revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; genetic data or biometric data when processed in order to uniquely identify a person; or data concerning health, sex life and sexual orientation – Art. 9(1).
11 www.hcch.net/en/projects/legislative-projects/judgments
12 A "first meeting" in June 2016 will consider preparation of a draft Convention - https://assets.hcch.net/docs/679bd42c-f974-461a-8e1a-31e1b51eda10.pdf paras 11-14.
13 The Hague Conference is considering an additional instrument on direct jurisdiction, including "exorbitant grounds" – fn. 11, para. 13.
14 See www.iicom.org/intermedia/intermedia-january-2016/dark-clouds.
15 To be discussed in a future *PL&B* article.
16 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

Survey on cloud accountability tools

The cloud accountability project is inviting organisations to take part in a short online survey to learn about the impact of accountability in the cloud and the expected value of accountability tools.

The EU General Data Protection Regulation requires cloud providers and customers to be more responsible with personal and sensitive data they are storing and processing in the cloud. Yet, how to become such a responsible data steward? The EU-funded A4Cloud project has developed various mechanisms and prototype tools.

For example, tools that help organisations to make conscious choices of the cloud services to use or tools that provide incident notifications to you and your customers.

• *The survey, based at Tilburg Institute for Law, Technology & Society, Tilburg University, the Netherlands, will take approximately 15 minutes. See www.a4cloud.eu/node/2457#sthash.Dj6op1p4.dpuf*

The changing landscape for data processors under the GDPR

Data processors must be prepared for more detailed contracts and liability for breaches of the GDPR, say **Lorna Cropper** and **Kate Pickering**.

Under the Data Privacy Directive 95/46/EU (the "Directive") data processors' obligations extend to providing processing with appropriate "technical security measures and organisational measures" and complying with any additional requirements as specified in any contract with the controller. While the definition of "processor" in the Directive and the General Data Protection Regulation (GDPR) are virtually the same, any similarities between the present and future legislation ends here as the above mentioned narrow set of requirements for data processors will widen extensively under the GDPR. For example, processors who were previously not subject to the Directive may need to be data protection compliant under the GDPR due to its increased territorial scope. Processors will also be accountable for demonstrating their compliance; they will be answerable to the supervisory authority (presently known as the data protection authority) and will need to adhere to the GDPR's requirements on data transfers to a third country or an international organisation. Data subjects will be able to issue legal proceedings against a processor and make a claim for compensation against them. Perhaps the most fundamental and potentially consequential change is that processors will also be subject to the sanctions that the supervising authorities will have at their disposal, including the much discussed increased financial penalties.

Increased territorial scope

Article 3 of the GDPR outlines the Territorial Scope of the regulation which applies to processors in the following scenarios:

1. an EU based processor acting for an EU based or non-EU based controller;[1]
2. a non-EU based processor engaged by an EU controller;[2] or
3. a non-EU based processor that offers goods or services or that monitors the behaviour of the individual on behalf of the controller.[3]

Accountability

While there may only be two overt references to accountability in the GDPR, one in the recitals and another at Article 5(2), the concept of accountability is threaded throughout the regulation both for controllers and processors. Fulfilling such obligations will necessitate much more administration for processors who will need to be able to evidence their data protection compliance. For example, Article 28(2a) specifies that processors must maintain written records "including in an electronic form" which detail "all categories of personal data processing activities carried out on behalf of a controller". The obligations equally specify that the records need to show, amongst other things, the name and contact details of each controller on whose behalf the processor is instructed, the categories of processing performed on behalf of each of those controllers, details of any data transfer to a third country or international organisation besides a general description of technical and organisational measures.

These requirements do not apply to an organisation with fewer than 250 employees unless the processing in question "is likely to result in a risk for the rights and freedoms of data subject (sic), the processing is not occasional, or the processing includes special categories of data".[4] The importance of maintaining these records cannot be underestimated as they need to be made available to the supervisory authority on request and may be taken into consideration where a processor's compliance is investigated.

Data Transfers

Under the GDPR, data processors will be legally responsible for transfers to a third country, i.e., a country outside the EEA, or for transfers to an international organisation. Responsibility is for both the initial transfer and any onward transfer. The possibility of transfers to third countries is broadened under the GDPR which permits transfers to a territory or specified sector on condition that the transfer destination ensures an adequate level of protection. In situations where the Commission has not provided an adequacy decision, a processor can transfer personal data to a third country or an international organisation on condition that the processor has given appropriate safeguards and there are "effective legal remedies for data subjects".[5]

The GDPR provides for a number of appropriate safeguards which are divided into two categories, namely those that do not require any specific authorisation from a supervisory authority and those that do. Appropriate safeguards which do not require any specific authorisation include EU standard contractual clauses (EU model clauses) and an organisation's Binding Corporate Rules, which are formally recognised as an option for data transfers under the GDPR. It is interesting to note that under the GDPR an approved code of conduct or an approved certification can evidence appropriate safeguards. These frameworks which can be used to demonstrate compliance for a number of GDPR provisions such as data protection by design and by default or security can only be used for data transfers on condition that the processor in the third country provides binding and enforceable commitments "to apply the appropriate safeguards, including as regards data subjects' rights".[6] This explicit reference to data subjects' rights, which is reiterated throughout the GDPR, highlights the importance which the EU has attached to personal data in today's ubiquitous technological

environment and tries to balance this against the transfer of data. It nonetheless underlines how important it is for processors to ensure that they have the necessary compliant measures in place when the GDPR comes into force.

Appropriate safeguards which a processor may wish to engage but which will require authorisation from a supervisory authority include contractual clauses, in addition to the EU model clauses, between the controller or processer and the controller, processor or recipient of the data in a third country or international organisation. Authorisation is also required for "provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights".[7]

Data processors' liability

Processors will be liable for breaches of the GDPR from:

1. data subjects who may sue processors directly;
2. regulators who may impose significant fines; and
3. controllers who may sue for breach of contract.

Processors may also be exposed to a claim from other processors or controllers with whom they share concurrent processing obligations and who have had to pay full compensation to a data subject for the damage suffered due to a breach of the GDPR. This is a significant change in a processors' potential exposure to liability which will, no doubt, have a significant impact on how processors and controllers and processors and sub-processors interact and enter into contractual relationships going forward.

Data subjects will be able to claim compensation for the unlawful processing of their personal information directly against controllers or processors. This is a slightly less comfortable position for processors, who have to date (for the most part), enjoyed their position in the shadows letting the controllers take on the statutory burden. Processors will be liable only for the damage caused by the processing where they have not complied with GPDR obligations specifically directed at processors or where they have not acted in accordance with the lawful instructions of the controller. Yet this matter is less cut and dried where a processor is involved in the same processing as either the controller or another processor and can be held liable for all of the damage. Where an action is brought solely against one processor despite other controllers and/or processors being involved, that one processor is entitled to a statutory indemnity against the other processors or controllers corresponding with the level of responsibility for the damage. While ultimately a processor may receive proportionate redress from other controllers and/or processors, the manner in which such payment is recovered may well be bureaucratic, logistical and time consuming.

Processors will therefore want to clearly describe their responsibilities in contracts with controllers and sub-processors, particularly where there are concurrent obligations, or alternatively work to ensure contractually, and in practice, that there are no, or limited, concurrent processing obligations. Controllers and processors alike will want a detailed understanding of processing operations, data flows, sub-processors and organisational security measures at the very least. It will be to all parties' advantage to keep detailed, readily accessible records of each party's own processing operations and respective compliance with the controller's instructions in order that each party is able to swiftly establish its position in the event of any breach. Such record-keeping would be supplemental to the requirements described above under accountability.

Contractual complexity

Data processors must be prepared for more detailed contracts, attempts by controllers and sub-processors to limit liability by way of contract and longer lead times when negotiating deals in order to carefully attend to data protection issues, especially in complex supply chain arrangements. The above possibilities provide the potential for a myriad of contractual issues not to mention protracted disputes when things go wrong. It will be interesting to see whether any guidance is produced on this by the EU Article 29 Data Protection Working Party or Data Protection Authorities as organisations begin their GDPR transition. In any event it would be commercially pragmatic for processors (and controllers) to make sure that they maintain the highest standards of data protection compliance which are regularly reviewed when the GDPR comes into force in order that any investigation does not find their systems and measures inadequate.

While codes of conduct and certification mechanisms mentioned above can act as a competitive differentiator for controllers and processors, they may cause additional burdens and/or responsibilities. For example, a controller with whom the processor has a long standing relationship may contractually oblige a processor to put a specific code of conduct in place.

Sanctions

The level of sanctions available to the supervisory authority has been headline grabbing since the Commission first published its draft of the GDPR in 2012. Any processor in doubt over the impact of the GDPR upon them needs only to consider the wording of Article 79(3 new)(a) which specifies the infringements of "obligations of the controller and the processor" which attract the lower scale administrative fine of up to €10 million, or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The higher level of administrative fines, which are up to €20 million and 4% respectively, could potentially be imposed on a processor who did not, for example, comply with the data transfer obligations under the GDPR.

Above is a selection of arguably the most onerous provisions within the GDPR for processors. What follows are details about several other responsibilities on data processors under the GDPR, which have been summarised for completeness and must be given appropriate attention by processors considering their GDPR readiness strategy.

Data Protection Officers

Processors will be required to appoint a data protection officer where the processing is carried out by a public authority or body (except for courts

acting in their judicial capacity), if the processing involves the regular and systematic monitoring of data subjects on a large scale or the processing is of sensitive personal data and data relating to criminal convictions and offences on a large scale.[8]

Breach notifications

A processor who becomes aware of a personal data breach must notify the controller without undue delay.

Co-operation and consultation

On request, processors must co-operate with the supervisory authority in the performance of its tasks. Prior to processing personal data, processors may need to consult the supervisory authority in certain cases to ensure effective protection of rights and freedoms of data subjects.

Sub-processing

Processors will not be able to subcontract their processing obligations unless the controller provides prior specific or general written consent. If additional processors are enlisted, they must be on terms of a written contract (or other legal act) that directly flow down the same (not just equivalent) obligations that are imposed on the data processor under its contract with the controller. Furthermore, processors will remain fully liable to the controller for the performance of data protection obligations by the other processors.

Data security

While obligations to have appropriate technical and organisational measures and to ensure a level of security appropriate to the risk will be familiar to processors, under the GDPR security measures are far more extensive. This is not surprising given the higher level of cyber security threats to organisations today and the regularity of data security breaches. The GDPR thus requests processors to consider appropriate measures such as pseudonymisation and encryption; the ability to restore the availability and access to data in a timely manner if a physical or technical incident occurs; and a system in place to regular review, assess and evaluate its security systems. It is also essential that processors have a comprehensive understanding of the type of data they process (particularly if sub-processors are engaged).

Processor not established in the EU

In certain circumstances where non-EU processors' activities relate to the offering of goods or services or monitoring the behaviour of the individual on behalf of the controller,[9] the controller or the processor shall designate in writing a representative in the Union.

Conclusion

The forthcoming GDPR applies to both controllers and processors and while commentators on data protection often inform us at length how it is the most important piece of data protection legislation in decades, the shift it will bring for processors of personal data is equally immense. It is important therefore that processors make themselves familiar with their new obligations under the GDPR and begin to consider their contractual arrangements with controllers, other processors and sub-processors while formulating their GDPR readiness strategy. Given the level of sanctions a supervisory authority can impose, to quote the exiting UK Information Commissioner, Christopher Graham, "There are 20 million reasons to get EU reforms right".

AUTHORS

Lorna Cropper, Senior Associate & Kate Pickering, Senior Associate, Fieldfisher LLP.
Emails:Lorna.Cropper@fieldfisher.com, Kate.Pickering@fieldfisher.com

REFERENCES

1 Article 3(1) General Data Protection Regulation..
2 *ibid*.
3 Article 3(2).
4 Article 28(4).
5 Article 42(1).
6 Article 42(2)(d) and (e).
7 Article 42(2a)(b).
8 Article 35.
9 Article 3(2).

Next UK Information Commissioner announced

The UK government announced on 22 March that Elizabeth Denham, Information and Privacy Commissioner, British Columbia, Canada, is the preferred candidate to be the UK's next Information Commissioner.

She is well known for her work internationally in the privacy and open government fields and was a speaker at PL&B's Annual International Conferences in Cambridge in 2014 and 2015.

The next step is a pre-scrutiny hearing by the Culture, Media and Sports Select Committee, approval by the Privy Council, and final approval by Her Majesty the Queen. This process is seen as a formality as the government says in its statement that 'Ms Denham will take over from current incumbent Christopher Graham in summer 2016.' His term of office ends on 28 June.

Baroness Neville-Rolfe, UK Minister for Data Protection, said: "The work of the Information Commissioner is vital for public and business alike. I'm pleased that we are recommending Elizabeth Denham to take on this role."

"She has a track record of working with business and other stakeholders, as well as a proactive approach to enforcing data protection law."

Information Commissioner designate, Elizabeth Denham, said: "I am honoured to be nominated for the position of Information Commissioner for the UK. I believe the rapid pace of technological change we face will continue to accelerate and present challenges to information rights – we must ensure access to information while maintaining high standards of data protection."

"The Information Commissioner's Office has a global reputation for practical, innovative and responsive regulation. I look forward to contributing to this work."

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK