27 YEARS
1987-2014

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Regulations bring Singapore's data privacy law into force

No 'whitelist' of countries for data exports exists, but the regulations allow for the use of Binding Corporate Rules. **Graham Greenleaf** analyses the situation.

On 2 July 2014, the data protection provisions of Singapore's Personal Data Protection Act 2012 (PDPA) came into force, following an 18 month transition period for companies to prepare for compliance.[1] (*PL&B International* February 2013 pp. 14-16 and June 2013 p. 34) To complete the process, the Personal Data Protection Regulations 2014 (PDPR) were made on 15 May 2014, the most important aspects of which concern data exports.

Data export regulations

Organisations to which the PDPA applies may not transfer personal data outside Singapore except in accordance with regulations. The Act requires the regulations "to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act".[2] The PDPR require that the transferring organisation ("the organisation that transfers the personal data from Singapore to the country or territory outside Singapore") must comply with the PDPA while it retains possession or control of the data (irrespective of where the data is located).[3] It must also[4] "take appropriate steps

Continued on p.3

Issue 130 **August 2014**

INTERNATIONAL report

ISSUE NO 130 **AUGUST 2014**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

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

SUB EDITOR
Tom Cooper

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

CONTRIBUTORS
Kwang Bae Park
Lee & Ko, Seoul, South Korea
Hwan Kyoung Ko
Lee & Ko, Seoul, South Korea
Robert Gellman
Washington DC, US
Allan Chiang
Office of the Privacy Commissioner for Personal Data, Hong Kong
Katharina A. Weimer
Reed Smith LLP, Munich, Germany
Robert Waixel
PL&B Correspondent
Merrill Dresner
PL&B Correspondent

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

Developments in Russia, Turkey, Singapore and Korea

Russian President, Vladimir Putin, has now signed the Internet law that requires Internet companies to store all personal data of Russian users at data centres within Russia. Also, Russia's Data Protection Authority is pressing the government for stronger sanctions (p.11). There are some signs in Turkey now that a DP law may emerge (p.28) as part of its bid for EU membership. Another area influenced by EU DP law is Latin America, where there is no common standard (p.16).

We also keep a close eye on Asia as there are constantly new developments – this time our Asia Pacific Editor and correspondents report on Japan (p.23), Singapore (p.1) and China (p.22). Watch this space for the *PL&B's* next Asia workshop in London, planned for the last week in May 2015.

The EU Data Protection Authorities, who at the end of July met with executives from Google, Yahoo and Microsoft, are concerned about the implementation of the European Court of Justice landmark ruling on Right to be Forgotten (RPBF). The DPAs put 25 detailed questions to the search engines and expect to issue guidelines by the autumn. In this issue, the Hong Kong Privacy Commissioner evaluates the global implications of the RPBF decision (p.18), and we report on what the Information and Privacy Commissioner of British Columbia, Canada, influential in Asia, has to say on accountability (p.30).

Both the EU and the US are making attempts to narrow down the privacy gap between the regions. The EU is willing to continue with the Safe Harbor programme subject to revisions (p.10) and the US has promised to guarantee EU citizens the same privacy rights as its own citizens have (p.7). The DP Regulations may now be adopted during 2015 (p.10).

The management story in this issue come from Angry Birds, which is keen to talk to regulators to avoid any problems now and in the future (p.14). Also, read on p.26 how Barcelona in Spain is developing a 'Smart City' with privacy constraints in mind. In Germany, DPAs have issued guidance on apps. While not ground-breaking, sometimes it is useful to know that nothing unexpected has been said (p.20).

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.

Foreigners' privacy rights in the US: Little more than a gesture

Recent promises have in fact little practical value as they would not create rights of access or amendment for records in exempt systems. By **Robert Gellman**.

In June 2014, the US Attorney General indicated that the Obama Administration would seek to amend the Privacy Act of 1974 to extend the Act's protections to EU citizens.[1] Currently, the Act protects only citizens of the United States and aliens lawfully admitted for permanent residence. Others – call them non-US persons – have no rights under the Act. At one level, the proposal to change the law is simple. However, in context, there may be less to it than appears on the surface. In order to appreciate the stakes, one needs to know more about the background and limitations of the Privacy Act as well as the options for changing the law.

Background

The Privacy Act of 1974[2] was one of the earliest national privacy laws and the first to implement formally Fair Information Practices.[3] The Act provides transparency, a right to access and amend records; limits on collection, use and disclosure; and other processing restrictions.

The Act covers federal government agencies and some government contractors. Unlike national privacy laws elsewhere, the Privacy Act of 1974 does not apply to state or local governments, private companies, or non-profits.

The key concept in the Act is system of records because most of the Act's requirements apply to systems of records. A system of records is a group of records from which information is retrieved by the name of an individual or other identifying particular. What is interesting about this definition is that the test is a factual one. If an agency maintains a file of personal information in alphabetic order but no one actually retrieves records by the name of the data subject, the file is not a system of records. This approach to determining whether privacy rules attach to personal information is meaningless today when computer records are retrieved with a few keystrokes.

Exemptions

Agencies can exempt some systems of records from some of the Act's requirements. There are two categories of exemptions, general and specific with each category having subcategories. No records are automatically exempt. An agency invokes an exemption by adopting a rule using familiar rulemaking procedures.

The Act provides two different subcategories of general exemption. First, the Central Intelligence Agency may exempt any system of records that it maintains, regardless of the nature or purpose of the records. Second, any agency can exempt records if it (or a component) performs as its principal function any activity related to the enforcement of criminal laws and the records are compiled for a criminal law enforcement purpose. Many records at the FBI and other law enforcement agencies qualify. A large number of federal agencies either are law enforcement agencies or have components with criminal law enforcement functions. The Department of Homeland Security exempted more than 40 systems of records under the general law enforcement exemption.[4] Exempted systems include some that affect travellers to the US and those seeking visas.

The scope of the general exemptions is quite broad. No agency can exempt a system from the public notice requirement or from the Act's limits on disclosure, but an agency can exempt a system from the requirement to provide access and amendment rights. Importantly, an agency using the general exemption can exempt a system of records from the civil remedies of the Act.

I want to emphasize that last point. A generally exempt system of records can be exempted from the provision of the Act that allows individuals to enforce their rights in federal court. For many years, the government argued that this provision prevents individuals from suing an agency over any violation of the few requirements that apply to exempt systems of records. In practice, the courts have not interpreted the provision that narrowly, and courts do entertain some Privacy Act lawsuits involving exempt systems of records.

An agency can also exempt a system of records from the Privacy Act under specific exemptions. There are seven subcategories of specific exemptions protecting specific interests including national security information. The most relevant specific exemption covers investigative material compiled for law enforcement purposes other than material covered by the general law enforcement exemption. Between the general and specific exemptions, the Act allows an agency to apply an exemption to nearly all law enforcement records.[5]

The specific exemptions are not as expansive as the general exemptions. An agency using a specific exemption can exempt a system of records from fewer provisions of the Act as compared with the general exemption. An agency can deny an individual access and correction rights under both the general and specific exemptions. However, the exemption from civil remedies is only available for generally exempt systems of records.

The Act's exemptions can be confusing to understand. The most important points for present purposes are:

1 Americans who have rights under the Privacy Act of 1974 find those rights severely limited if a system of records is exempt.
2 The Department of Homeland Security's (DHS) systems that are of particular interest to travellers to the US are generally exempt from many of the Act's requirements, including the right to file a civil lawsuit.
3 Virtually all law enforcement records have been exempted from the right of access and amendment under the Privacy Act. Most agencies invoke every available exemption for every system of records.

Effectively, there is no right of access or amendment under the Privacy Act to most law enforcement systems of records.

4 Agencies can deny and have denied the right to file a law suit over Privacy Act rights for criminal law enforcement systems of records.

I have to offer two balancing comments here. First, the federal Freedom of Information Act[6] (FOIA) allows any individual to ask for his or her own record.[7] Every individual has the same right to sue to obtain access to records. However, the FOIA only provides access to records. It does not create a right to ask for an amendment to a record, nor does the FOIA impose a requirement that records be accurate, relevant, timely, or complete.[8] The right to amend arises only under the Privacy Act. For access, however, the FOIA provides some enforceable rights.[9]

Second, some agencies grant non-US persons the ability to ask for access and amendment under the Privacy Act as a matter of policy (and not of right). DHS is one of those agencies.[10] Agencies that, as a matter of discretion, provide access and amendment opportunities can even extend those opportunities to exempt systems of records. Regardless, neither DHS nor the Privacy Act gives non-US persons the right to file a suit in federal court.

A meaningful right or a gesture?

What would change if Congress amended the Privacy Act to grant non-US persons the same rights as Americans? The answer is that non-US persons would gain no rights of access or amendment for records in exempt systems because American citizens do not have those rights. For generally exempt records, the Privacy Act allows agencies to deny anyone the right to sue in federal court.

Just about every law enforcement system of records is exempt from access and amendment. Every CIA system is exempt. Every intelligence system is exempt, if for no other reason than because intelligence systems are classified. DHS exemptions cover many of the systems of records that might be of interest to those travelling to the United States.

To be sure, some provisions in the Privacy Act might benefit non-US persons. Some non-exempt systems contain information about non-US persons. With an amendment, non-US persons would acquire enforceable access and correction rights with respect to those records. Non-US persons who travel to, go to school in, or do business in the United States may have Privacy Act records in government records.

The Act also has provisions beyond access and correction that might benefit non-US persons in the same way that the provisions benefit American citizens. In many instances, agencies that operate non-exempt systems already apply the same general privacy rules to all records in their systems of records. It is simply too complicated for agencies to separate out records from the same system of records based on citizenship and apply different policies. As explained above, agencies sometime respond to access and correction requests from non-US persons as a matter of discretion.

In the end, changing the Privacy Act to grant non-US persons the same rights that American citizens have would make remarkably little difference with respect to access and amendment of records. The privacy-affecting activities of the United States that attracted so much attention and raised so many concerns around the world recently create records that are almost certainly exempt from access and correction rights and from the ability to enforce rights in court. Other consequences of a change in the Act would likely have limited significance too.

So is the Attorney General's offer to seek a change in the law meaningful? At one level, it will change little that is of prime interest to EU citizens. However, at another level, granting the same privacy rights to non-US persons that American citizens have is a matter of fairness and equality. Americans generally have rights under foreign data protection laws. It is hard to find a justification for denying non-US persons rights under the major privacy law applicable to the federal government.

The EU may be willing to make concessions in other areas if the Obama Administration commits to seeking a change that grants non-US persons more rights. However, no one should assume that the change has much actual substance or significance to it. It is little more than a gesture.

Ways to change the Act

How might the Attorney General's offer to change the Act be accomplished? No specific proposal is on the table, but I see two main ways to do it.

First, the law could simply provide that all individuals, regardless of citizenship, have the same rights. That change would be simple to draft and simple to implement. However, the politics could be troublesome.

The issue of extending the Privacy Act of 1974 to cover foreigners came up quietly during my years on Capitol Hill, when I was a staffer principally responsible for the Act. There was no general interest in the idea and no pressure for change to the Act.

A few years ago, some Senators showed interest in amending the Privacy Act. An informal group of privacy advocates, agency insiders, and Senate staff worked on amendments. The effort eventually influenced a bill, (S.1732) introduced in 2011, which received no serious legislative attention.

During those informal discussions, the idea of extending privacy rights to non-US persons arose. Senate staffers immediately rejected the idea. They said that granting privacy rights to non-US persons would be viewed as granting rights to Osama bin Laden. They argued that no elected representative would vote for it. That ended the discussion.

Osama bin Laden is dead, but someone else could be a substitute here. Proposed bills sometimes become politically sensitive and sometimes not. The political characterization of an amendment depends on a host of often random factors. It is possible that support from the Obama Administration, privacy advocates, and American businesses seeking compromises with EU privacy regulators on the Safe Harbor Framework might succeed in pushing a proposal. On the other hand, there seems to be significant opposition from Republicans to almost everything that President Obama proposes. A Privacy Act amendment could become entangled in current political hot button immigration debates. It is hard to predict how the politics would play out in practice.

A RECIPROCITY APPROACH

A different approach would grant rights to citizens of countries that grant privacy rights to American citizens. A law that recognizes reciprocity might be easier to pass.

If this solves the immediate political problem, it presents others in its place. How can we tell which countries grants privacy rights to American citizens? For many countries, it is a simple judgment. EU countries, Canada, Australia, New Zealand, and many others have qualifying laws.

Yet even if it were easy to tell, we would still need a process to decide. Rather than have each US agency make its own determination, we might assign a single agency the responsibility to make the determination. The Office of Management and Budget would be the obvious choice because it has general responsibilities for providing guidance to agencies about the Privacy Act.

We can posit that countries will fall in one of three categories. For some countries, it would be easy to determine that American citizens have the same rights as their own citizens. For other countries, there might be no privacy law, and in those cases, citizens of those countries would be denied privacy rights under the Act.

Countries in the middle are more troublesome. One country might have a privacy law on the books, but there may be no implementation of the law in fact. Another country – if there are any that emulate the US so-called sectoral approach to privacy – might have a series of privacy laws, some granting rights to foreigners and some not. It might be harder to make determinations in these cases. Another possibility is that a country might grant privacy rights to American citizens that are not the equivalent of the rights granted under the US law. For example, a law might grant access rights but not correction rights. Or a law might not give foreigners the right to sue government agencies that withheld records.

In all cases, it might be necessary to develop standards to determine if a country's law met the standard. There is precedent here in the standard in the EU Data Protection Directive that allows export of personal data to a third country that ensures an "adequate" level or protection. Whether adequacy would really be a proper standard is far from certain. A privacy law is a complex bundle of elements, and weighing them all can be difficult.

Applying any standard presents its own problems. Some in the US have been unhappy about having anyone judge the degree of privacy protection in a nation's privacy laws. While some in the US try to argue with a straight face that American privacy laws meet EU standards, the reality is that American privacy laws are demonstrably weaker and less comprehensive than the privacy laws in any EU country. Regardless of the facts here, the controversy about having a standard and the content of that standard remains.

If the US established a general standard for judging foreign privacy laws to grant reciprocal rights, it would undermine arguments against the use of standards by others who judge our privacy regime. Could the US avoid the standard problem by just passing a law covering EU citizens? Sure, but that would run the risk of alienating Canadian, Australians, New Zealanders, and citizens of many other non-EU countries that have good privacy laws that protect Americans. This particular cure might be worse than the disease, and it might provoke responses from non-EU countries.

I do not mean to suggest that there is no possible solution to the Privacy Act implementation problem outlined here. Perhaps the all-foreigner approach would not attract political opposition in practice. Perhaps an adequacy standard would work, or we could use a simpler test for assessing privacy laws. We might even take the official word of another government whether the privacy law regulating government records protected Americans.

The point is that translating into statute the idea of granting privacy rights to foreigners under the Privacy Act is not simple. Once you move beyond the press release stage, the amendment to accomplish the objective requires some hard choices.

It is hard to predict whether an amendment to the Privacy Act of 1974 could actually pass. Both privacy groups and business groups are likely to support the proposed change, and an amendment could become law eventually. However, no EU citizen should expect any meaningful and enforceable rights even if it does.

REFERENCES

1 http://europa.eu/rapid/press-release_STATEMENT-14-208_en.htm
2 www.law.cornell.edu/uscode/text/5/552a
3 See Robert Gellman, *Fair Information Practices: A Basic History*, http://bobgellman.com/rg-docs/rg-FIPshistory.pdf
4 http://www.ecfr.gov/cgi-bin/text-idx?SID=bd3621259b5cc43767299bcba46b5226&node=6:1.0.1.1.2&rgn=div5#6:1.0.1.1.2.3.1.10.3
5 The specific law enforcement exemption has a limit if an individual is denied a right, benefit, or privilege. In that case, access (but not amendment) rights are granted except for the name of a confidential source. 5 U.S.C. § 552a(k)(2)
6 5 U.S.C. § 552, www.law.cornell.edu/uscode/text/5/552
7 The FOIA allows any agency that is part of the "intelligence community" to reject a request from a foreign government entity or a representative of a foreign government entity. 5 U.S.C. § 552(a)(3)(E)
8 See 5 U.S.C. § 552a(e)(5). Note that an agency can use the general exemptions to exempt a system of records from these record keeping standards
9 The exemptions under the FOIA differ from those under the Privacy Act. Under the FOIA, an agency can withhold any part of any record that meets a statutory standard for withholding. Under the Privacy Act, an agency must first exempt a system of records through a rulemaking before applying an exemption in practice. Also, some records exempt under the Privacy Act may be available under the FOIA, and vice versa. Most law enforcement records are, however, exempt under both laws.
10 See DHS Privacy Policy Guidance Memorandum, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-US Persons (Memorandum Number: 2007-1), www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

AUTHOR

Robert Gellman is a Privacy and Information Policy Consultant in Washington, DC.
Email: bob@bobgellman.com
www.bobgellman.com

Your Subscription **includes**

1. Six Reports a year
The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

2. Online search function
Subscribers can search the *PL&B* website to access: back issues since 1998; special reports, slides, videos and recordings from *PL&B* events.

3. Regular e-news
Subscribers receive updates about relevant news as and when it happens. Choose international and/or United Kingdom data protection news.

4. Helpline Enquiry Service
Subscribers can request information about the current status of legislation and other information.

5. Index
Search a country, subject and company index (1987-2014) www.privacylaws.com/Publications/report_index/

Electronic Option
The electronic PDF format enables you to: receive the Report on publication; click-through from email and web addresses; and follow links from the contents page to articles.

Subscription Discounts
Discounts for 2-4 users or 5-25 users and 2 years (10%) or 3 years (15%). See www.privacylaws.com/subscribe

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists.*

Privacy Laws & Business also publishes the United Kingdom Report, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

Single User Access

❑ *PL&B International* Report Subscription **£500**

❑ *UK/International* Reports Combined Subscription **£800**

Subscription Discounts

Discounts for 2-4 users or 5-25 users

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

Go to www.privacylaws.com/subscribe

Special academic rate – 50% discount on above prices – contact the *PL&B* office

Subscription Includes:

Six new issues of each report, on-line access to back issues, special reports, and event documentation.

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: sales@privacylaws.com 13/08

www.privacylaws.com

Guarantee

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