ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Facebook Belgium to comply with court's cookie decision

Multinationals face increasing pressure from DPAs. A Belgian court supported the Belgian DPA's record breaking 250,000 Euros per day fine on Facebook. By **Laura Linkomies** and **Stewart Dresner**.

The Brussels tribunal of first instance has issued an injunction against Facebook to stop it collecting personal data from non-Facebook users in Belgium[1]. The injunction[2], initiated by Willem Debeuckelaere, President, Belgium's Commission for the Protection of Privacy (DPA), was due to take effect within 48 hours after notification of the judgment which was published on 9 November.

Continued on p.3

The TPP Agreement: An anti-privacy treaty for most of APEC

Agreement facilitates international data transfers but brushes privacy to one side. By **Graham Greenleaf**.

Twelve Pacific-rim nations accounting for 40% of the global economy, including most significant APEC economies other than China, have reached agreement on a historic free-trade agreement, or are queuing up to join. The Trans-Pacific Partnership Agreement (TPP)[1] was signed in Atlanta, Georgia on 5 October at the conclusion of eight years of negotiation.

Continued on p.4

Issue 138 **December 2015**

INTERNATIONAL report

ISSUE NO 138 DECEMBER 2015

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

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

CONTRIBUTORS
Yuli Takatsuki & Phil Lee
Fieldfisher Silicon Valley, US

Xawery Konarski and Grzegorz Sibiga
Traple Konarski Podrecki i Wspólnicy sp.j, Poland

Francis A. Medeiros and Lee A. Bygrave
Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo

Chantal Bernier
Dentons LLP, Canada

Francis Aldhouse and Liz Upton
Bird & Bird, UK

Kwang Bae Park
Lee & Ko, South Korea

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

End of year does not mean Regulation finale

We continuously hear messages from Brussels that the EU DP Regulation will be adopted by the end of this year (p.17). However, even if political agreement is found, both the European Parliament and the Council need to organise a vote before the final text is published.

The EU DP draft Regulation includes provisions on anonymization. In Norway, the DPA has issued guidance that echoes the previous work by the EU Article 29 Working Group (p.18). The DPA says that by employing anonymization techniques, the processing of data falls outside the scope of the law.

In October, we attended the Privacy Commissioners' International Conference in Amsterdam and learned about the privacy bridges that are being developed to fill the gap between Europe and the US (p.10). EU DPAs need to cooperate more under the future EU DP regime (p.8). But the DPAs say they are ready – and they already sometimes tackle the big multinationals together. Read about Belgium's action on Facebook on p.1. Also, changes towards more harmonisation, such as Poland's amendments to the law to facilitate use of BCRs and standard contractual clauses, help the DPAs to have a consistent approach (p.12). The next issue on the EU legislative agenda may be the revision of the EU e-Privacy Directive. Something needs to be done, says former UK Deputy Data Protection Commissioner, Francis Aldhouse (p.24).

The TPP agreement is not just about trade – it includes provisions that aim to facilitate a global framework for free flow of information, but with insufficient privacy protections, says our Asia-Pacific Editor, Graham Greenleaf (p.1).

In the US, the surveillance regime has been reviewed. Companies that need to understand US government requests for data can find invaluable advice on p.14. Our reports from Asia cover the most recent legislative developments in South Korea (p.26) and an analysis of enforcement in Hong Kong, where the first direct marketing fines have now been issued (p.21). In Latin America, more and more countries are adopting data protection laws, mostly due to commercial pressures (p.19), writes Chantal Bernier, Canada's former Interim Privacy Commissioner, reporting from the Ibero-American network meeting in Montevideo, Uruguay.

Finally, season's greetings from all of us at PL&B and a Happy New Year!

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.

Facebook... from p.1

The company faced a fine of 250,000 euros per day payable to Belgium's DPA. What happened next provides an example of a strategic battle between the huge US-based tech firms and the European DPAs on how the law should be interpreted.

The (un)necessary cookie?

The Tribunal ruled that Facebook's practice of putting cookies on devices of non-Facebook registered users visiting Facebook violates Belgian data protection law. According to Facebook, the datr cookie is necessary for security reasons.

Belgium's DPA had published on 16 May 2015 a statement which provides the basis for this case[3]. It stated "Since January 2015 the privacy commissions of the Netherlands (the lead authority), Hamburg-Germany and Belgium have worked together as an own-initiative group. France and Spain recently joined the contact group… Up to this day Facebook refuses to recognize the application of Belgian legislation nor the Belgian Privacy Commission."

Importantly, the Tribunal ruled, following the view of Belgium's DPA, that Facebook is subject to Belgian DP law for all its activities in Belgium. Facebook's lawyers argued in vain that Facebook organises its European activities entirely from its establishment in Dublin, Ireland. Consequently, according to Facebook, it only needs to take into account the Irish data protection legislation under the supervision of Ireland's Data Protection Authority. But the judge rejected this argument and referred to the decision of the European Court of Justice in the Google Spain case as a precedent.

If the decision of the Brussels tribunal is followed in other EU Member States, DPAs in these Member States will now also claim that they are competent to supervise Facebook's activities in their territory. In practice, this would mean that, as long as European data protection law is not entirely harmonised, Facebook would need to take into account all 28 different data protection regimes in the EU.

Facebook says it has changed its practice for non-Facebook users accessing Facebook so that it will comply with the Belgian Tribunal's 9 November decision. This means that anyone without a Facebook account in Belgium will now have to create an account to be able to log in to Facebook to view content.

The strategic battle for Facebook users' support

Will Facebook prevail in its claim that its use of a datr cookie will track the users whether they are Facebook members or not? Facebook has argued that the use of this cookie provides better security for Facebook users as the risk of accounts being hijacked diminishes.

Facebook's spokesman said: "We had hoped to address the [Belgian Privacy Commission's] BPC's concerns in a way that allowed us to continue using a security cookie that protected Belgian people from more than 33,000 takeover attempts in the past month. We're disappointed we were unable to reach an agreement and now people will be required to log in or register for an account to see publicly available content on Facebook. We expect the BPC to apply these restrictions across the web, which could restrict Belgians' access to websites with maps, videos, share buttons, and similar content."

A lawyer representing Facebook stated in the court proceeding that "Belgium will become the cradle for cyber terrorists."

The Belgian DP Commission has commissioned an academic study which examined Facebook's claims in detail[4]. This study challenges Facebook's claim that the main objective of the datr cookie is to ensure data security and repel Denial of Service attacks. Facebook claims that they need to follow all Facebook users to ensure that they are trustworthy and detect and repel Denial of Service attacks.

However, the study suggests that the underlying commercial purpose is to track all visitors' subsequent travel around the Internet for two years following their last contact with Facebook so that advertising can follow the visitor according to their interests as expressed by the websites they have visited and the social media they have used.

Whereas people with Facebook accounts are more likely to understand this process, visitors to Facebook who do not have an account, are unlikely to understand the implications of their visit, as the privacy policy relevant to them is on page 10 of a 10 page policy and even clicking on a Facebook "like" button or choosing a language option is considered an opt-in according to Facebook's procedure.

Facebook states that they monitor IP addresses not individuals, but the European Court of Justice has ruled that IP addresses are, in effect, personal data (ECJ C-70/10, recital 51).

The strategic battle for Facebook's users support is that Facebook, in its implementation of the Belgian DPA's order, effectively bars non-account users in Belgium from Facebook Belgium's public services. This may well have the effect of encouraging their sentiment against the DPA's decision, in effect using public opinion to challenge the law as interpreted by the DPA and the tribunal.

Facebook would prefer that the case is heard in Ireland and has said that it will appeal the decision.

Ireland's DPA's view

A spokesman from Ireland's Information Commissioner's office told PL&B: 'The office of the Data Protection Commissioner is satisfied that it has jurisdiction over the personal data processing activities of Facebook Ireland Ltd on the basis of its establishment here and that the Irish Data Protection Acts 1988 and 2003 apply. A claim to exclusivity of jurisdiction has never been made by the Irish authority not least because up until recently European data protection authorities cooperated to route the majority of complaints and queries through the Irish authority. A number of cases, however, have been considered in relation to Facebook Ireland Ltd's activities by other European data protection authorities (Germany and France in particular) which have asserted jurisdiction and

Facebook...continued on p.29

TPP... from p.1

The TPP is primarily an agreement 'to establish a free trade area',[2] an agreement which 'will strip thousands of trade tariffs in the region and set common labour, environmental and legal standards among signatories'.[3] But it is also the first legally-binding agreement affecting data privacy that has been entered into by APEC members, although it is not formally an APEC (Asia-Pacific Economic Cooperation) instrument. The APEC Privacy Framework (2004), like all other APEC 'agreements', is not legally binding on its parties. In contrast, the TPP is a real international agreement, with enforcement provisions.

The TPP only imposes the most limited positive requirements for privacy protection, but imposes stronger and more precise limits on the extent of privacy protection that TPP parties can legally provide. The principal aim of this article is to explain these provisions and their overall effect on privacy protection.

The parties, now and future: A treaty for almost all of APEC, perhaps beyond

All twelve initial parties to the TPP are APEC member economies: Australia; Brunei Darussalam; Canada; Chile; Japan; Malaysia; Mexico; New Zealand; Peru; Singapore; the United States; and Vietnam. Four more APEC member countries have stated they wish to join the TPP: Indonesia, the second most populous country in APEC;[4] South Korea, the third-largest economy in East Asia;[5] as well as Taiwan;[6] and the Philippines.[7] That leaves just five of the twenty-one APEC member economies not involved at present. Neither China nor the Hong Kong SAR, both APEC members, are parties to the TPP,[8] although significant opinion-makers in China are open to joining the TPP.[9] The other 'missing' APEC member economies are Papua New Guinea, Russia and Thailand.

It is still speculative whether, and when, the TPP will come into force. The final drafting of the document will not be completed for at least a month.[10] The US Congress will then have three months to review it before it votes whether or not to support it. Every other party will also need to go through any domestic processes required for ratification, possibly including enacting legislation. Many politicians on both sides of US politics have expressed opposition to the TPP, and there is still some opposition in Japan.

Scope limited to measures affecting trade

Chapter 14 (Electronic Commerce) applies to 'measures adopted or maintained by a Party that affect trade by electronic means', so the scope may be much broader than measures that govern or 'apply to' trade.

However, it does not apply to 'a) government procurement; or b) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection' (Article 14.2.2). Although government owned or controlled enterprises may be subject to the TPP,[11] this provision creates exclusions. It will for most purposes exclude the collection or processing of information by or on behalf of governments, reinforcing that the provisions only apply to 'trade by electronic means' and not all processing of information by electronic means. This means, for example, that legislation requiring local storage and processing of government information is exempt from the TPP. In such cases, there is no need to consider the data localisation restrictions in Article 14.13.

The scope of any privacy protection required is further limited to only some private sector activities by Article 14.8, next discussed.

Weak data protection requirements

Article 14.8 ('Personal Information Protection') is the only TPP provision requiring some positive protection of personal information, other than the direct marketing provision.

For the purpose of 'enhancing consumer confidence in electronic commerce',[12] (but without any mention of protecting human rights) Article 14.8.2 requires that 'each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. This legal framework need only apply to 'users of electronic commerce'. It need not apply to all private sector activities (even if commercial), nor to categories of private sector personal data such as employee information. Public sector personal data need not be included unless it comes within 'electronic commerce', and even then might fall outside Article 14.2.2 discussed above.

As to what type of 'legal framework' will suffice, a note to Article 14.8.2 specifies that '[f]or greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy'. This last clause seems to be written with the US Federal Trade Commission in mind. Given that a 'legal framework' is required, mere self-regulation would not appear to be sufficient, which is an advance on the APEC Privacy Framework.[13] However, since a 'measure' is defined to include 'any … practice' (Article 1.3), as well as laws, even this is not completely free from doubt.

Article 14.8.2 also requires that 'in the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies'. However, no specific international instruments are mentioned, and there is no list of principles included in the TPP. Nor are any specific enforcement measures mentioned. These absences make the 'legal framework' required by the Article completely nebulous.

Article 14.8.5 provides that 'Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks.' The APEC Cross-border Privacy Rules Scheme (CBPRs) purports to be such a

mechanism, but the 'autonomous' recognition of EU 'adequacy' status, or recognition under other 'white-list' approaches could also constitute such 'recognition of regulatory outcomes'.

Article 14.8.3 requires that '[e]ach Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction'. 'Non-discriminatory practices' is not defined, but would presumably include a requirement that data privacy laws should not limit their protection only to the citizens or residents of the country concerned, as was once the case with privacy laws in countries such as Australia, and is still proposed in India. In any event, the inclusion of 'shall endeavour' removes any force from this provision, as does 'shall encourage' in Article 14.8.5.

Direct marketing limitations

Parties are required to take measures (which need not be laws) regarding unsolicited commercial electronic messages, to facilitate recipients preventing their ongoing receipt (opt-out), or requiring consent to receipt (opt-in), or otherwise providing for their minimisation. They must provide 'recourse' (which is not required for general privacy protection) against non-compliant suppliers, and shall endeavour to cooperate with other Parties (Article 14.14: Unsolicited Commercial Electronic Messages). Brunei, which does not currently have a data protection law, is given time to comply.

Restrictions on data export limitations

'Cross-Border Transfer of Information by Electronic Means' is addressed in Article 14.11. It first recognises 'that each Party may have its own regulatory requirements concerning the transfer of information by electronic means' (Article 14.11.1). It then requires that cross-border transfers of personal information be allowed when this activity is for the conduct of the business of a service supplier from one of the TPP parties.[14]

Any exceptions from this obligation to allow personal data exports must be justified under Article 14.11.3, which allows such a restrictive measure only if it satisfies four requirements: i) it is 'to achieve a legitimate public policy objective'; and ii) it 'is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination'; iii) it is not applied so as to be 'a disguised restriction on trade'; and iv) it 'does not impose restrictions on transfers of information greater than are required to achieve the objective'.[15]

Alleged failure to meet any one of these requirements in this 'four-step-test' could result in a country's data export restrictions facing dispute settlement proceedings. This four-step-test is typical of conditions to allow exceptions in trade agreements, and is not an extreme restriction on data exports or localisation (at least not compared with what might have been included). For example, the aim of obtaining a positive 'adequacy' assessment by the European Union could be argued to be a 'legitimate policy objective'. However, it is of concern that these requirements might create a 'regulatory chill',[16] particularly when coupled with ISDS provisions (as discussed below).

> Each Party may have its own regulatory requirements concerning the transfer of information by electronic means.

Prohibitions on data localisation

Edward Snowden's revelations and the European Court of Justice[17] have confirmed that personal data cannot be protected against US agencies once it is located on US servers. One response is for a country to require that some categories of data be only stored and processed on local servers ('data localisation').

The TPP deals with data localisation in much the same way as data export restrictions: a prima facie ban, subject to tough tests to overcome the ban. Its anti-data-localisation provisions are in Article 14.13 ('Location of Computing Facilities'), which follows a similar approach to the data export provisions. First, formal acknowledgment is given to each Party's right to have its own 'regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications' (Article 14.13.1). 'Computing facilities', for this Article, only include those 'for commercial use'.[18]

Then, a TPP Party is prohibited from requiring a service supplier from one of the TPP parties (a 'covered person') 'to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory' (Article 14.13.2). In other words, data localisation is prima facie banned. Then, the same 'four-step-test' of justification for any exceptions is applied as was the case for data export limitations.[19]

Russia's data localisation requirements would have little chance of passing these tests, if it became a TPP party. Data localisation requirements in the laws of Vietnam and (if it joins TPP) Indonesia will have to meet the four-step-test or breach TPP.

Both the data export and data localisation provisions are subject to exceptions in the lists of Non-Conforming Measures (NCMs) accepted for each State party. There are no specific NCMs for articles 14.11 or 14.13, but they could be affected by exceptions phrased in general terms for some States.

Dispute settlement

State parties to the TPP can use Chapter 28's dispute settlement provisions involving specially constituted panels, to resolve disputes concerning interpretation or application of the TPP. Potentially of greater importance are the procedures in relation to investment disputes under Chapter 9 ('Investment'), and the possibility of Investor-State Dispute Settlement (ISDS) provisions being used. Most of these provisions pose few problems for

privacy protection. A breach by a party of the data export limitation and data localisation provisions will not automatically trigger entitlement to ISDS provisions by affected companies in, say, the USA (Article 9.6.4).

> The ISDS possibilities should frighten every country that has a data privacy law but has a smaller litigation budget than Google or Facebook.

The most significant investment protection relevant to data privacy is the prohibition of direct or indirect expropriation of investments,[20] except for a public purpose and for payment of fair and prompt compensation (Article 9.7.1). Failure to compensate will lead to the threat of ISDS procedures. However, what if the main benefit to a company in the US, in setting up e-commerce facilities in another country, was the transfer of personal data to the US where data privacy laws posed far less interference in what could be done with the data than under the laws of that country? Could breaches of the data export limitation or data localisation provisions then constitute an indirect expropriation of the investment? The ISDS possibilities should frighten every country that has a data privacy law but has a smaller litigation budget than Google or Facebook.

This may not cause countries that already have data export restrictions to rush to water them down, but any party that is considering enacting new or stronger data privacy laws (including any data localisation) will have to give some very serious thought to the possibilities of actions, particularly ISDS actions. They may also need to draw breath before embarking on any strong enforcement of existing laws, for fear of an ISDS reaction.

Conclusions: A Faustian bargain

These TPP requirements seem to embody the type of binding international privacy treaty that the US (in particular) wishes to achieve: a) no substantive or meaningful requirements to protect privacy; b) coupled with prohibitions on data export limitations or data localisation requirements that can only be overcome by a complex 'four-step-test' of justification; and c) backed up by the risk of enforcement proceedings between states or under ISDS provisions, both involving uncertain outcomes from dubious tribunals[21] and potentially very large damages claims. This approach is consistent with the 2013 revisions to the OECD privacy Guidelines,[22] but with much sharper teeth.

For the US, it is a great deal: no need to worry about how strong local privacy laws in other countries may be (that battle is largely lost anyway, with 109 countries already with data privacy laws[23]), because it will now be more difficult to prevent most personal data from being exported to the US, where such laws do not significantly impede commercial use, and where state surveillance also has wide reign. Perhaps there are TPP signatories other than the US aiming to be net personal data importers, or who explicitly don't care about to which overseas countries their own citizens' personal data is exported, but they are difficult to identify.

For all the other states whose personal data will be 'hoovered up', it is more likely to be a Faustian bargain: put at risk the protection of the privacy of your citizens (except at home) in return for the golden chalice of trade liberalisation. TPP may mean no enforceable requirements of privacy protection, but enforceable free flow of personal data, and a one-way flow at that. For privacy, it is a poor bargain. The main problem with the TPP is that human rights such as privacy protection should not be bargaining chips in trade agreements, where they require that states decide what their protection is worth compared with greater access to trade in bananas.[24]

The strength of this argument depends on the extent to which the two four-step-tests (satisfaction of which will now be required to justify data export restrictions or data localisation requirements), coupled with the prospect of ISDS actions, will have the consequences of regulatory chill and regulatory roll-

back that I predict and fear. There can be reasonable arguments that they will not. But should this risk be taken?

The TPP is the first multilateral trade agreement with detailed provisions relating to privacy protection. If the TPP is defeated in the US Congress, this will be a net gain for privacy protection, whatever one thinks about the other potential economic advantages of the TPP. The TPP's privacy-related provisions reflect US interests to a considerable extent. It remains to be seen whether future multilateral trade agreements will contain similar provisions.

ACKNOWLEDGEMENTS

Valuable comments have been received from Prof Nohyoung Park, Prof Leon Trakman, Chris Connolly, Professor Lee Bygrave, Professor Sanya Reid Smith and Blair Stewart. All content remains the responsibility of the author.

REFERENCES

1 New Zealand Foreign Affairs & Trade 'Text of the TPP Agreement' <http://tpp.mfat.govt.nz/text>
2 TPP, Article 1.1.
3 Nick O'Malley ' The Trans-Pacific Partnership: Pacific countries agree to historic trade pact' The Sydney Morning Herald , 6 October 2015 http://www.smh.com.au/business/the-economy/tpp-deal-pacific-countries-agree-to-historic-trade-pact-20151005-gk1vq2#ixzz3ruWzAAic
4 'Indonesia will join Trans-Pacific Partnership, Jokowi tells Obama' The Guardian 27 October 2015.
5 Jessica J Lee 'The Truth About South Korea's TPP Shift' The Diplomat, 23 October 2015 <http://thediplomat.com/2015/10/the-truth-about-south-koreas-tpp-shift/>
6 Executive Yuan 'Taiwan determined to join TPP' 27 October 2015.
7 Reuters 'Philippines' Aquino wants to join Trans-Pacific Partnership', 14 October 2015 <http://uk.reuters.com/article/2015/10/14/uk-philippines-trade-tpp-idUKKCN0S80WJ20151014>; see also Prashanth Parameswaran 'Confirmed: Philippines Wants to Join TPP', The Diplomat, 25 June 2015 <http://thediplomat.com/2015/06/confirmed-philippines-wants-to-join-tpp/>
8 Macau SAR, the other Chinese territory which has a data privacy law, is not an APEC member economy.
9 Reuters 'China communist party paper says country should join U.S.-led trade pact', 24 October 2015 <http://www.reuters.com/article/2015/10/25/us-china-trade-tpp-idUSKCN0SJ01X20151025#2GF0PVwz1pTAh15m.99>
10 ibid
11 TPP Article 1.3, definition of 'enterprise': 'enterprise means any entity constituted or organized under applicable law, whether or not for profit, and whether privately or governmentally owned or controlled, including any corporation, trust, partnership, sole proprietorship, joint venture, association, or similar organization.'
12 TPP Article 14.8.1: 'The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce'.
13 G Greenleaf Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP, 2014), p. 36.
14 TPP Article 14.11.2: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person'. See also Article 14.1, definition of 'covered person'.
15 TPP Article 14.11.3: 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and b) does not impose restrictions on transfers of information greater than are required to achieve the objective."
16 Luke Nottage and Leon Trakman 'As Asia embraces the Trans-Pacific Partnership, ISDS opposition fluctuates' The Conversation (Australia) 20 Nov 2015 <https://theconversation.com/as-asia-embraces-the-trans-pacific-partnership-isds-opposition-fluctuates-50979>
17 Maximillian Schrems v Data Protection Commissioner (6 October 2015) Court of Justice of the European Union, Judgment in Case C-362/14
18 TPP Article 14.1 definition 'computing facilities means computer servers and storage devices for processing or storing information for commercial use.'
19 TPP Article 14.13.3: 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective. '
20 TPP Article 9.7.1: 'No Party shall expropriate or nationalise a covered investment either directly or indirectly through measures equivalent to expropriation or nationalisation (expropriation) …'
21 Hill, above.
22 Greenleaf Asian Data Privacy Laws, Ch 19, section 3.1 'Revised OECD privacy Guidelines 2013'.
23 G Greenleaf, 'Global data privacy laws 2015: 109 countries, with European laws now in a minority' (2015) 133 *Privacy Laws & Business International* Report, 14-17.
24 'This is not bananas we are talking about' said Spiros Simitis, 'Europe's de facto privacy doyen', when discussing EU/US tensions over the 1995 EU privacy Directive, cited by Lee Bygrave 'International agreements to protect personal data', J Rule and G Greenleaf (Eds) Global Privacy Protection: The First Generation, Edward Elgar, 2008, p.15.

Fate of EU data retention debated

EU's Justice and Home Affairs Council, which met 3-4 December, says that it has held a general discussion on the consequences of the invalidation of the Data Retention Directive by the European Court of Justice in April 2014.

'All member states considered that retaining bulk electronic communication data in a generalized manner is still allowed. A majority of delegations also considered that an EU-wide approach has to be considered in order to put an end to the fragmentation of the legal framework on data retention across the EU, and invited the Commission to present a new legislative initiative whenever possible.'

• *See http://www.consilium.europa.eu/en/meetings/jha/2015/12/03-04/*

GDPR to enhance DPA cooperation – What are the obstacles?

Laura Linkomies reports from Amsterdam on the PHAEDRA project findings and stakeholders' reactions to the proposed General Data Protection Regulation (GDPR).

Data Protection Authorities (DPAs) are keen to improve practical co-operation but face challenges in terms of sharing information and coordinating enforcement action. These findings are based on the EU-funded PHAEDRA project, which studied how to improve practical and helpful co-operation between Data Protection Authorities. The researchers from Trilateral consultancy have now summarised the interviews conducted with EU DPAs between April-May 2015. Topics covered included the main developments on the proposed draft General Data Protection Regulation (GDPR), including the consistency mechanism; One-Stop-Shop and European Data Protection Board; and their impact on cooperation between the 28 DPAs in the European Union.

Future cooperation under the Regulation

This mechanism under the GDPR is planned to ensure a coherent application of the provisions and would have an important supervisory role for the European Data Protection Board (EDPB) in case there are differing views amongst DPAs. As there is no final text yet, some DPAs did not comment on this issue in the interviews. Others thought that it was "the best possible compromise", or were doubtful about the speed of the process, clarity of the rules, increase of workflow and how this system can be made understandable to citizens. Speaking at the 37th Data Protection Authorities' International Conference side event, David Barnard-Wills, Partner at Trilateral consultancy, said that some DPAs envisage European level cooperation to be part of their daily lives in the near future. But cooperation requires formal mechanisms, he said.

Jacob Kohnstamm, President of the Netherlands' DPA, said that DPAs are not yet ready for the new model of cooperation under the GDPR. But the One-Stop-Shop will help. He hoped that the final text would reflect the European Parliament's text on this issue. "There should always be just one captain. The European Data Protection Board (EDPB) should have the status of a legal person," he said. This would mean that its decisions would be binding. He also said that the DPAs need more resources – the GDPR will be a complete failure if DPA budgets are not dramatically increased to cope with the extra demands on their work load.

Karolina Mojzesowicz, Head of the Reform Sector, the European Commission, explained where the Trilogue negotiations were at (end of October). She said that the negotiations were on track and that the European Parliament is fairly happy with the Council's general approach. A compromise is sought between 'having one captain' and the individual DPAs in the One-Stop-Shop. "Cases that come to the EDPB for its binding opinion should be exceptional. The DPAs already cooperate much now – this is very much how the consistency mechanism will work," she said.

She told the audience that the EDPB should be a lightweight structure with a Chair who is part-time and a Secretariat.

Wojciech Wiewiórowski, Assistant European Data Protection Supervisor, said that there are some practical issues to be solved. The EDPS would provide the Secretariat for EDPB, which in his view could only deal with 12-15 cases per year. "I was sceptical about Article 29 DP Working Group before. This group cooperates well but there are also situations where this readiness does not exist. In the Weltimmo case (*PL&B International Report*, Oct 2015, p.1), the Slovak and Hungarian DPA flagged the issue but other DPAs were not interested. Now we have an important ECJ decision".

He also said that opening up the GDPR now would not make sense – 'we will not be able to create a better system now. Most of the practical solutions will come from DPAs and national courts.'

Practical issues with cooperation

Steve Wood, Head of Policy Delivery, the UK Information Commissioner's Office, said that cooperation is needed behind the scenes even when there is no formal cooperation procedure. He said that the GPEN alerting tool had now been launched and that eight authorities have formally signed up to the system (p.11). We need trust – there are security concerns even if the system uses encryption, he said. The parties have signed a Memorandum of Understanding on confidentiality. "This is a two-way system. There are tools to share information but we also learn from each other. Participants can control who they share data with, for example only selected DPAs."

Wood explained that sometimes information is also shared about methods of working in the Article 29 DP Working Party context, for example with the recent GPEN sweep on children's data, DPAs exchanged views on the definition of a 'child'. This is particularly useful for smaller DPAs, he said.

Ignacio Sanchez from the EC Joint Research Centre spoke about the technical challenges involved: his research project organised a simulation of a pan-European data breach in order to evaluate responses. He is now analysing the results on how DPAs share information. DPAs do not often agree how information can be shared securely, he said. Common ground needs to be found and technical solutions can be of help.

The panellists were asked what will change in light of the recent Schrems and Weltimmo decisions (on invalidating EU-US Safe Harbor and on the applicability of EU data protection

law, *PL&B International Report* October 2015, p.1). Wojciech Wiewiórowski said that the Schrems case stresses the independence of DPAs, but what is a local case? At the moment, 95% of cases are local or national.

The EU Commission published on 6 November an explanatory Communication on the consequences of the Schrems ruling setting out guidance on international data transfers: http://ec.europa.eu/justice/newsroom/data-protection/news/151106_en.htm

The burning language question

A discussion followed about the difficulties surrounding the choice of language. Especially smaller DPAs with minority languages could face difficulties if the cases to be referred to the EDPB would have to be translated. Also, which EU languages would be possible to use? EDPS Assistant Supervisor, Wojciech Wiewiórowski, said that in his view, they should either accept all 23 EU languages or just one. However, some DPAs, regardless of their size, manage to navigate in the jungle of several different languages. Tine A. Larsen from the Luxembourg DPA said that they routinely work in English, French and German. She said that the authority often receives cooperation requests from other DPAs as many international companies are based in Luxembourg. In fact, 75% of their caseload are cross-border cases. But this creates problems in terms of confidentiality, she said. The Luxembourg DPA has learned over the years to take advice from other DPAs so as not to duplicate effort.

It was thought that it would be confusing for individuals if they bring a case in one Member State and receive a response in another language – national procedures need to happen in the national language(s).

> National procedures need to happen in the national language(s).

Floriane Leclercq, Secretary of the Francophone DPO Association, said that they mainly work in French but maintain contact with other networks too.

What after the reform?

Sophie Kwasny, Head of Data Protection Unit, from the Council of Europe, said that the CoE modernisation process has been slightly delayed due to the GDPR – they are waiting for the outcome of the Trilogue. The cooperation aspect is important – the Council will look into Convention 108 provision on mutual assistance so that it will not be an obstacle.

Endre Gyozo Szabo from Hungary's DPA said that DPAs need to harmonise enforcement actions. "We are excited about the EDPB. We are heading into the unknown and will lose one aspect of our independence but DPAs need to stay together." He said that as a practical example of cooperation, the Article 29 DP WP is now working on a single complaint form.

Artemi Rallo from the University Jaume 1, Spain (and Spain's former DP Commissioner) said that solidarity is needed; the DP community is now in two camps – there are 8-10 leading authorities and the rest. But most of the new tools under the GDPR need all the DPAs, he said. Some DPAs just do not have the resources to become involved in Article 29 subgroups, for example, and therefore will not have as much influence as some other countries. This is not a question of language but money, he explained.

David Barnard-Wills said that DPAs recognise the need for cooperation but work needs to be done post-GDPR. Some are preparing for new aspects of the Regulation whilst other have a 'wait and see' approach.

Paul de Hert, Professor at Vrije Universiteit Brussels said that the overall feeling is that stakeholders want to make the most of the DP reform. Can we learn lessons from how the Schengen computer system works? There will be an issue with languages, but also with the sense of autonomy of DPAs and interdependence, he said.

WILL THE EU DP REGULATION HARMONISE DATA PROTECTION IN THE EU?

Extract from the PHAEDRA study:

The extent to which the GDPR will harmonise data protection in the EU is still debated. Some DPAs interviewed expressed opinions that the Regulation's provisions would mean European DPAs had equivalent powers and roles, reducing the diversity of national implementations of data protection law, in effect creating a single regime of data protection. Others instead expressed the belief that there would still remain differences in national practice and particularly in both culture and strategy, as well as differences in size, resources, experience and economic context in which they were required to operate as a regulator. A requirement emerging from this may be the need to better understand where there will be remaining differences in areas not covered (and therefore not harmonised) by the GDPR.

Related to this is a practical debate about the extent to which structure and formalisation can contribute to more effective co-operation and co-ordination between European DPAs. For a minority of DPAs, the creation of structured systems for information exchange, shared complaint handling strategies, templates, forms, alerting systems, etc. were likely to be necessary given the scale of co-operation under the GDPR. For another minority, such systems were seen as problematic, in that they either reduced the operational flexibility of DPAs and their ability to respond to the particular context of a particular case, or they believed that agreement on such structures would not be possible given the remaining diversity between DPAs, even under the GDPR. For most DPAs structure and formalisation could be potentially helpful in various areas, either increasing efficiency, serving as a check or reminder for processes, and increasing harmonisation. Many reminded us that structured systems would always need to be flexible enough to cope with unanticipated events and requirements.

• *See http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2_D1_20150720.pdf*

DPAs try to find solutions for EU-US international transfers

Self-regulatory attempts resulted in 'privacy bridges' that are a bottom-up approach towards closing the gap between the parties. **Laura Linkomies** reports from Amsterdam.

The 37th International Privacy Commissioners' Conference, held in Amsterdam at the end of October, concentrated on discussing a study that was commissioned specifically for this conference on EU-US international data transfers[1]. The high calibre working group was somewhat unlucky that the revolutionary European Court of Justice Schrems decision, invalidating the EU-US Safe Harbor agreement, was issued just at the time the group had finished its work. But then on the other hand, the work was never about solving problems with Safe Harbor, but seeking alternative solutions whilst waiting for a new international instrument.

Opening the conference, the President of the Netherlands' Data Protection Authority, Jacob Kohnstamm said: "The privacy Bridges project presented realistic first steps to build practical bridges that make the lives of people, companies, governments and supervisory authorities, who have to deal with different legislative systems, a little easier. The steps are small, but essential first steps for a higher level of privacy protection".

The working group said that social and technological realities in the EU and the US are closer than the legal differences suggest.

Most of the open part of the conference was dedicated to discussing the bridges in order to find out from stakeholders whether they thought them viable, and to enrich these ideas. Not everyone was happy, though. Civil society representatives voiced some harsh criticism, and some others thought that the suggestions did not amount to anything new or substantial. However, several interesting ideas emerged during the mini-workshops organised around the different 'bridges'.

Practical steps to bridge the gaps between EU and US

The proposed bridges are:

1. Formalising the working relationship between the EU Article 29 Working Party and the US Federal Trade Commission
2. User controls
3. New approaches to transparency
4. User-complaint mechanisms: Redress to privacy violations by services outside a user's own region
5. Government access to private sector personal data
6. De-identification of personal data
7. Best practices for security breach notification
8. Accountability
9. Greater government-to-government engagement
10. Collaborating on and funding for privacy programmes.

At the conference, the privacy bridges Co-Chairs, Nico van Eijk and Daniel Weitzner explained the rationale behind the work. They said that the working group did not seek to comment on the Safe Harbor, EU regulation or surveillance, but sought to provide a bottom-up approach to transfers.

David Weitzner said: "We hoped to find a way to have a collaborative relationship between the EU and US, both at governmental and business level. Unfortunately we had finished our work by the time the Safe Harbor decision came out. But now we have a basis to avoid the kind of collapse of trust that has taken place".

EU Commissioner, Věra Jourová , welcomed the report and said that technological tools are needed – the project provides inspiration to look for practical ways to implement data protection rules. The final result on the EU DP Regulation is expected by the end of this year. The EU and US need to reach mutual understanding of each other's privacy cultures, she said.

Hiroshi Miyashita, Professor at law, Chuo University, Japan said that we need to adopt every bridge which had been proposed. Jose Alejandro Bermudez from Nymity's Latin American branch said that most bridges are indeed applicable globally, and especially those on cooperation and investigating data breaches. But a US non-governmental organisation, Digital Rights, said that the focus should be on fundamental rights – the report has been written just to fit US participants. Bojana Bellamy, President of Hunton & Williams Centre for Information Policy leadership, and participant in the bridges project, said that the group has done what it can – it could not legislate on privacy.

Article 29 Group and US FTC

The bridges working group proposed that the two parties would sign a Memorandum of Understanding (MOU), suggesting that there would be a system in place for informing each other when starting to investigate an important new policy question. In the end it was thought that this was too much and the parties would start with organising a joint workshop.

"This may have been a bridge too far," Jacob Kohnstamm said. He explained that the FTC currently organises stakeholder workshops in the US that bring together industry, academia and government. "That does not happen in Europe or such discussion take place in confidence." He thought the best approach would be now to organise a joint event and formalise the arrangement later.

Daniel Weitzner, Co-Chair of the privacy bridges project, said that it would be very fruitful to have these transatlantic discussions about future privacy challenges, for example on autonomous cars. Another area identified as a potential was drones as they also involve aviation issues and therefore need to be looked at from different angles.

Giovanni Buttarelli, European Data Protection Supervisor (EDPS), said that he appreciated the exercise to make practical suggestions. "But to prepare for the future we need a new deal." Individual user control is the key, he said. "The data Protection community should be less conservative and look into the future," he said.

Safe Harbor deliberations

Isabelle Falque-Pierrotin, President, the CNIL, France's Data Protection Authority and Chair of the EU Article 29 Working Party, said that we need a better awareness of civil society as the balance has tilted towards industry. On Safe Harbor, she said that the Article 29 Working Party wants to be pragmatic, but they are bound by the ECJ decision. "All stakeholders have to take responsibility. We need to negotiate an intergovernmental agreement, Safe Harbor number 2, or a more political agreement. As DPAs we are in a transitory period. We will carry on with other instruments while giving the actors time to find a solution. If nothing has been agreed by the transition period, DPAs may resort to enforcement action," she said.

She said that industry also has to take responsibility and organise their data flows differently. Edith Ramirez, Chair, the US Federal Trade Commission said that the FTC is urging companies to do much more in this area. "We will organise soon a workshop on how users are being tracked," she said. She explained that the media has been looking for differences between the EU and US regimes in terms of the Schrems decision, but in reality there are many commonalities. The FTC is committed to further cooperation with the EU even if there were no Memorandum of Understanding. For example, a person from the CNIL will start a secondment within the FTC. She also said that enforcement agencies need to engage with other regulators who have not previously dealt with data protection issues.

Giovanni Buttarelli encouraged other countries, and not just the US, to modernise their data transfer arrangements. We will have a new scenario by 2018, he said, referring to the EU DP Regulation. There will be a need for global partnership, he said.

Conclusion

Previous Netherlands Data Protection Data Protection Commissioner and ex-EDPS, Peter Hustinx, summarised the feedback from the workshops. He said that the role of technology was recognised, as well as the need for a new user interface – individuals need to be educated on privacy so that they can control their data. He said that there is a need to learn from cross-border data breaches. Some sort of clearing house would be useful but where would it be located? He thought that a EU-US MOU in not necessarily needed as cooperation is already underway. Joint workshops should be easy enough to organise.

"All bridges have been endorsed to larger or smaller degree," he said. But he asked about next steps and who would drive the project forward.

Jacob Kohnstamm explained in a separate press conference that members of the project will continue discussions and may report back later, perhaps some time in 2016. The Netherlands will take on the EU Council Presidency in 2016 and will include drones on the agenda – it is necessary for the EU and US to have a dialogue in this field to create a successful drone market. But there is of course also the ethics element.

He said that Bojana Bellamy will be the lead for the bridge on accountability. The participants from academia had to formalise their collaboration and proposed a price for the best privacy research proposal. Other actions will follow, he said.

REFERENCES

1 https://www.privacyconference2015.org/wp-content/uploads/2015/10/Privacy-Bridges-Paper-release-version.pdf
2 The GPEN website, showing many members, is at https://www.privacyenforcement.net/
3 https://www.privacyconference2015.org/dutch-dpa-signs-agreement-gpen-alert-system/
4 https://icdppc.org/participation-in-the-conference/global-cross-border-enforcement-cooperation-arrangement-list-of-participants/

REPORT FROM THE DPAs' CLOSED SESSION

The DPAs welcomed Benin, Georgia, Mexico and Ukraine as new members to the conference.

They adopted a Resolution on Privacy and International Humanitarian Action, and a communication on genetic and health data. The latter says that the use of genetic data could lead to a variety of risks, such as hacking and disclosure of intimate familial relationships, as well as ethnic discrimination, denial of services because of genetic predispositions, and other malicious uses. The DPAs propose more cooperation between data protection and scientific communities.

The DPAs also adopted a resolution on data protection oversight of security and intelligence. While DPAs do not have a direct enforcement role in terms of intelligence and security activities, most have roles including that of ombudsmen, auditors, consultants, educators, negotiators and policy advisers. The DPAs, therefore, say that each authority has to find its own way to contribute to the discussion, by promoting proportionality and lawfulness in intelligence activities, and establishing links with local and international oversight agencies. DPAs could also provide special assistance to oversight agencies while retaining their independence. Also, they can promote more transparency and wider use of encryption.

On international enforcement cooperation, the DPAs reported that eight DPAs have agreed to exchange information by using the GPEN[2] Alert System. Through this system, privacy authorities from all over the world can exchange information on a confidential basis about cross-border issues in specific cases. The aim is to further enhance the international cooperation in the area of privacy enforcement. The eight authorities which have signed up for the Beta version of the Alert Tool are: The Netherlands, Australia, the US FTC, Canada, Ireland, New Zealand, Norway and the United Kingdom[3]. In addition, ten DPAs formalised enforcement cooperation by signing an agreement.[4] The membership is the same as for the GPEN information exchange group, without the US FTC, Norway, and New Zealand, but adding Hong Kong, Estonia, Gibraltar, Isle of Man and Hungary.

New regime for data transfers from Poland to third countries

An amendment to the law facilitates use of BCRs and standard contractual clauses, no longer requiring a permit from GIODO, Poland's DPA. By **Xawery Konarski** and **Grzegorz Sibiga**.

On 1 January 2015 an amendment to the Personal Data Protection Act[1] came into effect in Poland and significantly changed the existing regulations. These modifications affect mainly the rules under which information security administrators perform their tasks and the conditions of personal data transfers from the territory of the Republic of Poland to a third country.

This article presents the new data transfer rules, while describing the essence of the amendment and the practice of Poland's personal Data Protection Authority (GIODO – Inspector General for Personal Data Protection). It should be noted here that the Polish legislator was inspired by the provisions of the draft of the EU General Data Protection Regulation. The liberalisation of existing rules is of great practical importance as Poland is one of Europe's leading outsourcing hubs (including, for example, Business Process Outsourcing (BPO) and IT services) and a major part of those services are provided to recipients (groups of companies) from third countries. It has also turned out that, with respect to transfers to the United States, the amendment has partially filled the legal gap which emerged after the judgment of the Court of Justice of the European Union (CJEU) in the Schrems case (*PL&B International Report* Oct 2015, p.1), as the new provisions permit data transfers under standard contractual clauses, without the need to apply for GIODO's consent.

New Rules v. Old Rules

The amended act has preserved the rule that in order to warrant the legality of a personal data transfer to a third country, such country must ensure adequate protection in its territory (Article 47.1). Such adequacy may be confirmed in two ways – either in a decision issued by the European Commission (Commission's finding) or in the course of a "self-assessment" carried out by the controller. In the latter case, such assessment is subject to scrutiny by GIODO to verify whether it is correct. However, under the Polish act, GIODO is not given any power to confirm the adequacy of protection (national finding), therefore the Polish authority cannot issue any certificates to this end.

If a third country does not offer adequate protection, the controller may resort to three "lines of support" to find a legal basis for data exports.

First, he may refer to one of the exceptions listed in Articles 47.2 – 47.3 of the Polish act, which reflect the derogations enumerated in Article 26.1 of EU Data Protection Directive 95/46/EC.[2]

As the next option, the controller may use standard contractual clauses, as approved by the European Commission pursuant to Article 26.4 of Directive 95/46/EC, or Binding Corporate Rules (BCRs), as approved by GIODO. This possibility has been added by the recent amendment. Its purpose is to introduce a rule under which the use of such instruments, which safeguard the interests of data subjects, releases the controller from the obligation to obtain a permit for data transfer (Article 48.2). It is a fundamental change since before that amendment had come into effect the controller was obliged to apply for a data transfer permit to GIODO even if he applied standard contractual clauses or BCR. Moreover, it was previously a common understanding that the fact that the controller has signed an agreement on the basis of standard contractual clauses does not obligate GIODO to consent to the transfer of personal data to a third country. Now such a risk is considerably reduced, as the controller is neither required to apply for such a permit nor even obliged to notify GIODO of any data transfers (to be) executed on that basis.

The third, and last, "line of support" at the controller's disposal is a procedure to apply for consent to GIODO. This scenario should be opted for where a data transfer cannot be executed under any of the previously described rules. GIODO gives such consent as an administrative decision. In accordance with Poland's laws, it should be given within 30 days, however GIODO often extends this time limit. This results, among other things, from the specific framework of proceedings carried out by GIODO, which examines, among other things, the technical and organisational safeguards which the data importer has in place.

As the new amendment has considerably contributed to the establishment of a new status of standard contractual clauses and BCRs, we will focus on the practical aspects of application of these instruments.

Model Clauses and BCRs

The primary advantage of the new regulations is the limitation of the legal risk to which the controller is exposed. GIODO is now bound both by the contract clauses approved by the European Commission and by his own decisions approving Binding Corporate Rules. This binding force means that GIODO may not challenge the use of such clauses or rules as an effective legal basis of data transfers. On the other hand, however, it should be noted that such data protection instruments are subject to the general principle that compliance with other (general) provisions of the Personal Data Protection Act is a *sine qua non* for admissibility of personal data transfers to a third country and, to that extent, GIODO may always put a halt to a transfer (eg. marketing data transfers despite the fact that the data subject has exercised the right to object to the processing of his data for this purpose). GIODO may also stop a transfer, as an exception, in any cases specified in decisions of the European Commission approving standard clauses. Such a situation may occur where, for example, GIODO becomes aware that the data importer (recipient) has failed to adhere to such clauses.

Standard Clauses

At present, all three sets of clauses are in common usage in Poland, ie. those approved by Commission Decision 2001/497/EC (controller-to-controller clauses), Commission Decision 2004/915/EC amending Decision 2001/497/EC (controller-to-controller clauses), and Commission Decision 2010/87/EU (controller-to-processor clauses). They are applied to data transfers both within a group of companies and between entities which are not members of the same group.

In practice, the most acute practical difficulties, and especially regarding data transfers as part of IT projects, including cloud computing, arise in the case of sub-outsourcing of data processing. As a result, two groups of factual states may be distinguished, depending on whether or not Decision 2010/87/EU is applicable.

The first group includes those cases where a processor established in a third country passes the data to another entity, established in the same or a different third country. If this is the case, such sub-outsourcing is banned unless it is approved, *a priori* and in writing, by the controller, which should be informed in relevant detail about a given sub-outsourced service provider and about the purpose and scope of such sub-outsourcing. Hence, practice developed in Poland does not depart from the solution adopted in Decision 2010/87/EU.

The second group covers those situations where data sub-outsourcing to an entity established in a third country is performed by a processor from the European Economic Area (EEA) or where a processor established in a third country transfers data received from a subcontractor established in the EEA to another entity. In such a case, the standard clauses annexed to Decision 2010/87/EU do not apply. In practice, the solution preferred by GIODO is an agreement between the controller from Poland and a subcontractor, to be entered into either directly or via the processor, which acts as the legal representative (attorney) of the controller.

BCRs

The amended Polish act has introduced a model of approval of binding corporate rules (BCR) by GIODO by way of an administrative decision (Article 48.3). However, the act does not specify the content of the BCR or any elements of the application for their approval. Nonetheless, there is no doubt that the relevant documents of the Working Party are fully applicable in this regard, and especially Article 29 of Directive 95/46/EC (WP 74, WP 133, WP 108 and WP 153-155), which clarify the requirements that any set of BCR should meet.

The Polish act does not set out any BCR examination criteria to be applied by GIODO, and, in particular, it is not clear which personal data safeguards are applicable, i.e. whether only those introduced by Directive 95/46/EC or those implemented by both European and national laws. This is a vital issue as some provisions of the Polish act require higher protection standards than the EU regulations. We believe the former approach is correct.

As regards the BCR approval procedure, two cases should be distinguished. In the first case, approval by GIODO is required for the Binding Corporate Rules prepared for a group of companies having its principal registered office in Poland.[3] GIODO acts here as the so-called lead authority, which is obliged to coordinate the works carried out by a corporation to adopt its BCR.[4] This is clearly provided for in Article 48.4, which sets out that prior to approval of the Binding Corporate Rules GIODO may consult competent Data Protection Authorities in those countries – members of the European Economic Area in the territory of which the relevant undertakings from the subject group of companies have their registered offices, while providing those authorities with any information that may be necessary to this end. And Article 48.5 obliges GIODO to take the outcomes of such consultations into consideration.

Nevertheless, considerably more weighty controversy has arisen concerning the solution adopted in the amended act for those sets of BCR that have been previously approved in another Member State of the European Union. In accordance with the Polish act, approval by GIODO is also required in this case (Article 48.5). This Polish regulation, which lacks any equivalent in the legislations of other EU Member States, leads to the situation where a corporation (group of companies) is expected to file once more, in Poland, the same application for approval of its BCR, which have already been approved in another Member State. This model is against the guidelines issued by the Article 29 Data Protection Working Party, which has unambiguously emphasised that it should be enough when such a procedure is carried out only once, ie. approval by the Data Protection Authority in one of the Members States will suffice (see, for example, WP 74, p. 20). Moreover, under the Polish act, GIODO is allowed, at the stage of examination of already approved BCR, to acknowledge decisions issued in other states. Therefore, we suggest that Poland's Data Protection Authority should work out a practice of simplified examination of already approved sets of BCR, without amending their content, as otherwise it would be possible that a group of companies has two different sets of BCR, i.e. one approved by GIODO and one approved by the Data Protection Authority in another Member State.[5] And this would be contrary to the idea of a uniform BCR for the entire group.

AUTHORS

Xawery Konarski, Senior Partner, and Grzegorz Sibiga, Of Counsel at law firm Traple Konarski Podrecki i Wspólnicy sp.j.
Emails: xawery.konarski@traple.pl; grzegorz.sibiga@traple.pl.

REFERENCES

1 The Act of 29 August 1997 on the Protection of Personal Data (unified text: Journals of Laws of 2014, item 1182 with amendments).
2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
3 To the date of publication of this article, the first application for approval of "Polish" BCR is still underway.
4 To the date of publication of this article, no decision (approval) of a "Polish" BCR, based on the new provisions, has been made and first application is still underway.
5 It seems that this approach has been taken by the Polish DPA that approves "foreign" BCR (ie. already approved in another EU country) in an automatic manner.

Getting to grips with US government requests for data

Phil Lee and **Yuli Takatsuki** provide Part 2 of their analysis by looking at access requests for law enforcement purposes, and say that cloud-based data is particularly vulnerable.

The legal framework that controls US government access to individuals' data is much talked about within European privacy circles. There is a commonly-held belief that the US framework is ill-defined and insufficiently protective of individuals' privacy rights. Yet despite this, many European privacy professionals, when pushed to explain this belief, find themselves forced to admit they know little about how US government data requests actually work.

That explains the purpose of this article, which is the second in a two-part series that seeks to clarify, in simple terms, the principal mechanisms by which US government authorities can obtain access to individuals' data from providers of communications or other cloud-based services. The first part in this series, published in the October edition of *Privacy Laws & Business International* Report, explained the US government's powers to access data in the context of national security. This part now explains the US government's powers to access data in the context of law enforcement requests.

One slight note of caution: this article discusses the issues at an intentionally high level. Its author is not a US attorney, but rather a European privacy lawyer who has encountered this issue in the context of representing US clients dealing with government requests for data on a regular basis. In that sense, you can think of this article as a "101" introductory overview about US government access to data – but there is naturally more complexity and detail than this article can convey within the limited space available.

Methods for compelling data disclosure

US law enforcement authorities (LEAs) have at their disposal three primary means to compel service providers to disclose their customers' data: subpoenas, court orders and warrants. Precisely which means is appropriate in any given context depends on the type of data sought and the statutory authority under which it is requested.

The key legislative authorities governing access to data are described below but, before discussing those, it is important first to understand the differences between a subpoena, court order and warrant, and how these determine what data may be obtained by an LEA. The differences are as follows:

- **Subpoena**: Of the three means for compelling a service provider to provide access to its customers' data, a subpoena is the easiest for an LEA to obtain. It can be issued by a duly-authorized government official, meaning that it does not (necessarily) undergo any kind of prior judicial review. Because it is easier to obtain, and generally has no judicial oversight prior to its issuance, the data that can be obtained by a subpoena is meant to be less privacy intrusive in nature than that which can be obtained through a court order or search warrant (for the most part, limited to a customer's subscriber information – such as name, address, length of service and means of payment).
- **Court order**: A court order is, as the name implies, an order issued by a court compelling, or prohibiting, specific action(s) by the person named in the order. In the case of law enforcement access to data, a court order compels a service provider to give an LEA access to its customers' data. A court order is judicially reviewed before issuance, and is therefore more difficult to obtain than a subpoena. In particular, the requesting LEA must show "specific and articulable facts" demonstrating "reasonable grounds" to believe that the data sought is "relevant and material to an ongoing criminal investigation". Being harder to obtain, a court order provides access to more privacy intrusive data than a subpoena – though is still mostly used to access non-content information (such as the customer's usage or purchase records – eg. the "from", "to" and "date" fields of an email, but generally not the contents of the email).
- **Search warrant**: A search warrant is the most privacy intrusive way to gain access to data. It must be issued by a judge or magistrate, and a requesting LEA must show "probable cause" that the data sought relates to a crime (contrast this with the lesser standard of "reasonable grounds" required to obtain a court order). As well as providing access to exactly the same types of non-content information as a subpoena or court order, a search warrant also permits access to the content of communications – whether stored or real-time communications. Service providers will often require LEAs to obtain a search warrant before they will permit LEAs access to their customers' content – though, in certain specified cases, the law does technically allow LEAs to access content with only a court order (see the '180 day' rule discussion below).

LEA tools to realize access to data

Having understood the means by which LEAs can compel access to data, it is important next to understand the tools available to LEAs to realize access to data. These tools essentially fall into two main categories – those that enable access to stored data or communications and those that enable interception of real-time data or communications.

In terms of access to stored data or communications, LEAs may either enter premises directly in order to search and seize data processing equipment (provided they have a search warrant) or, alternatively, compel a service provider to disclose specified customers' data (the precise data disclosed depending on whether the service provider is compelled by subpoena, court order or warrant).

In terms of intercepting real-time data or communications, LEAs may intercept non-content (eg. the user's IP address or the recipient of a communication) by using a 'pen register' device (a tool for intercepting outgoing communications) or a 'trap and trace' device (a tool for intercepting incoming communications). Alternatively, and generally only if they have a warrant, they may intercept the real-time content of a communication (eg. the content of an e-mail or a phone call) by means of a wiretap.

Constitutional protection against "unreasonable search and seizure"

Unlike Europe, where citizens have a fundamental right to a private life and to data protection under the EU Charter of Fundamental Rights, American citizens' do not enjoy a similar constitutional right to privacy. The closest protection that exists under the US Constitution is the Fourth Amendment, which provides:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Commonly referred to as the "prohibition against unreasonable search and seizure", the Fourth Amendment sets the rule that LEAs may only enter a person's premises and seize their effects (including their computers and other data processing equipment) with a search warrant issued upon demonstrating "probable cause". In other words, if an LEA needs access to communications and other data held on an individual's personal computer, they must obtain a search warrant.

The rules for data held in the cloud by service providers are somewhat different though. In that context, LEAs are typically not looking to search and seize a service provider's data processing equipment; they are instead looking to have the service provider itself disclose the data to the LEA.

As a consequence, a search warrant is not constitutionally required to obtain data from cloud service providers – and this is a significant point of concern for many privacy advocates, who argue that personal data in the cloud should benefit from the same constitutional protection as personal data on an individual's computer.

Instead, for cloud data, a search warrant is required for cloud-based data only to the extent expressly required by the Electronic Communications Privacy Act – the principal legislation controlling LEA access to data held by service providers.

The Electronic Communications Privacy Act

Originally brought into effect in 1986, the Electronic Communications Privacy Act (ECPA) has been criticized over the years for being overly-complex and out-of-touch with modern technology.

The overriding concern with ECPA is that it was passed in a very different technological era – before, even, Europe's Data Protection Directive, at a time when mobile phones were not in existence and no one had heard of the Internet, let alone cloud-based email or social networking. Whilst it might have been well-designed for the technological environment it was intended to address at the time, technologies have moved on.

One example is the ECPA's so-called '180 day rule' – where LEAs can potentially gain access to the content of communications without a warrant (only a court order) if they have been stored by a service provider for more than 180 days, whereas access to the content of communications less than 180 days' old requires a warrant. That rule perhaps made sense back in 1986, at a time when individuals did not store years' worth – even decades' worth – of their emails and files online; viewed in current times, it seems at best like a curious antiquity and, at worst, like a dangerous loophole. If applied strictly, it could in theory allow LEAs access to the majority of individuals' content data in the cloud without a warrant.

When it was adopted, ECPA consolidated and updated earlier legislation governing access to both stored and real-time communications. Structurally, it consists of three titles, being:

- **Title I (aka the Wiretap Act)** – this title sets the rules governing real-time interception of the contents of communications by wiretap. As discussed above, real-time interception of communications contents requires a search warrant.
- **Title II (aka the Stored Communications Act)** – this title sets the rules governing access to stored communications and data held by a service provider, including both content and non-content. As discussed above, the means by which a service provider can be compelled to provide access to this data may be a warrant (for access to content) or a court order or a subpoena (generally used for access to non-content). The Stored Communications Act does not apply to data stored on an individual's personal computer. For that, a search warrant would be required under the Fourth Amendment.

  A pen register, or dialled number recorder, is an electronic device that records all numbers called from a telephone line. A trap and trace device shows which phone numbers have called a phone to all incoming phone numbers.
- **Title III (Pen Register / Trap and Trace provisions)** – this title sets the rules governing real-time non-content interception of communications by using pen register and trap and trace tools (for outbound and inbound communications respectively). It can be thought of as the mirror complement to the real-time content interception provisions under the Wiretap Act. Use of a pen register or trap and trace requires an ECPA court order.

	Stored	Real-time interception
Unassisted search and seizure	Fourth Amendment *Search warrant*	ECPA Title I: Wiretap Act *Search warrant*
Non-content	ECPA Title II: Stored Communications Act (2703(c)) *Subpoena or Court Order (depending on data sought)*	ECPA Title III: Pen Register / Trap & Trace *Court Order*
Content	ECPA Title II: Stored Communications Act (2703(a)(b)) *Search warrant (or Court Order if >180 days)*	ECPA Title I: Wiretap Act *Search warrant*

The diagram above summarizes the types of data that might be sought by LEAs, the constitutional or statutory authority under which they may seek access, and the means by which they can compel access.

Summary: Guiding principles for businesses

As will be apparent from the above, far from being little in the way of available law governing LEA access to data, US law actually provides a wealth of legislative and constitutional controls. The precise data that can be accessed, and the means by which access may be compelled, depends on a number of factors, including whether the data sought is content or non-content, held on a personal computer or on a service provider's servers, stored or in transit, and its age.

In terms of guiding principles for businesses handling LEA access to data, the following are paramount:

- Decide whether you will respond to voluntary requests to data from LEAs, or whether you will provide data only if compelled. Ideally, adopt a global position on this – don't have different standards from country-to-country.
- Have in place a policy for handling LEA data disclosure requests. Make sure staff are educated about what to do when they receive a request and, in particular, to whom a request should be escalated.
- If compelled to disclose data, make sure that the means of compulsion used is correct for the data sought (eg. that a subpoena is not used to access data for which a court order is required). Be prepared to challenge any data disclosure orders that are inappropriate, overly-broad or vague.
- For valid orders, disclose only the minimum amount of data compelled. Do not disclose more data than compelled, eg. in the interests of being helpful – doing so may be a breach of law.
- Make sure your privacy policy discloses that you may share data with LEAs and the basis on which you may do this (eg. compulsion versus compliance with voluntary requests).
- Consider publishing transparency reports indicating the volume of LEA data requests received, appealed and complied with each year. This extra layer of transparency will be welcomed by your customers.

AUTHORS

Yuli Takatsuki, Director & Phil Lee, Head of US Office, Fieldfisher Silicon Valley, US.
Emails: Yuli.Takatsuki@fieldfisher.com and Phil.Lee@fieldfisher.com

book reviews

Privacy on the ground: Driving corporate behaviour in the United States and Europe

By Kenneth A. Bamberger and Deidre K. Mulligan

The authors of this book explain what drives corporations to adopt privacy practices, the role played by the law, and how these actions are manifested in practice. Starting at *Privacy Laws & Business's* Annual International Conference in Cambridge in 2010, corporate behaviours were assessed through interviews and questionnaires in five different countries: Spain, the US, France, the UK and Germany.

There are some surprising findings, such as that German and US companies approach privacy protection in much the same way. In both countries privacy professionals are relatively autonomous and participate in senior level strategic decision making. In Spain and France, firms tend to focus on meeting formal data protection requirements. In the UK, the response was more mixed. While privacy "principally derives from the law", the degree of operationalisation was not nearly as high as in Germany and the US.

The authors say that the extensive interviews with privacy professionals (54 DPOs were interviewed in depth, as well as 26 privacy lawyers and DPAs) show the limitations on the law's influence on corporate practices. Reality in the day-to-day business world can be quite different from legal requirements. The success of US and German DPOs suggests that assigning specialist privacy professionals is a helpful first step towards compliance with the law.

There is much merit in the authors' proposals for policymakers: 'bring the outside in' by supporting broad legal mandates, accountability and a privacy community consisting of advocacy groups, privacy experts, professional associations and labour representatives. This growing outside pressure pushes firms to fund and develop their privacy practices.

The book has a fresh approach into evaluating how privacy works on the ground, and the empirically inspired analysis will be of interest to any DPO or CPO in Europe or the US.

Published by the MIT Press
ISBN: 978-0-262-02998-8
338 pages Price £26.95

Reviewed by Laura Linkomies

EU DP Regulation Trilogue agreement by the end of the year still possible

Věra Jourová, European Commissioner for Justice, said at Forum Europe's 6th Annual DP and Privacy Conference in Brussels on 10 December that the EU Data Protection Regulation is in its "final stages… The European Commission will support its implementation… Business in Europe will save 2.3 billion Euros in administrative costs. It will develop new opportunities. We expect to arrive at an agreement in the next two weeks and then prepare for implementation… DPAs will work together more closely".

She described her personal commitment and involvement. "Yesterday I had breakfast with Mr Schrems. The Safe Harbor had deficiencies… We want robust safeguards for citizens. I met Julie Brill [US Federal Trade Commissioner] last Friday." Jourová said that business is looking for guidance on international transfers so the European Commission responded by issuing its recent Communication. We are waiting for the US Congress to adopt the Judicial Redress Act 2015 which would give European citizens the same rights as US citizens regarding the Privacy Act 1974. "The appropriate US Senate committee is discussing this subject today. I met the committee's chairman when in Washington recently."

In answer to *PL&B's* question, Věra Jourová said that the European Commission "will conduct continuous monitoring" of any new Safe Harbor system. It expects any new SH to have "a precise description and clear exceptions… to ensure that companies' commitments are fulfilled… The Commission will play a more active role". She will expect annual reports from:

1. Companies which are members of a new Safe Harbor
2. The US government on the scope of surveillance in the national security area, and
3. US-based Non-Governmental Organisations (NGOs) public interest organisations, which are advocating privacy as a fundamental right.

In future, there will be a clear suspension clause which has been only implicit in the past.

Julie Brill said the efforts of Congress to adopt the Judicial Redress Act 2015 are very significant.

PL&B asked how this proposed new law would give EU citizens rights in the US which would bridge the gap between:

- The narrow focus of the US Federal Privacy Act 1974, covering personal data held by the Federal government, and
- The broad scope of the EU Data Protection Regulation covering all types of personal data in which US citizens would have very broad rights in the EU.

The objective of reciprocal rights would be fulfilled only in part. Paul Nemitz, Director, Fundamental Rights, DG Justice, told *PL&B* that the Umbrella Agreement on police and national security data is neither an adequacy decision nor a legal treaty. "Equivalence is a problem with all agreements with the US, for example, the passing of personal data from the Federal government to the States. Even if the Judicial Redress Act is passed, it is not a perfect world, but it is progress."

Luxembourg's Justice Minister, Felix Braz, representing the EU Presidency, said that his team is working towards a conclusion of the Trilogue by 17 December. He said that "the new rules will be waterproof". The Luxembourg Presidency "wants to achieve high profile compromises" to achieve a Trilogue agreement by the end of the year.

EU Cyber Security Directive brings in data breach notification for many sectors

The EU Trilogue on the Network and Information Security Directive, the so-called Cyber Security Directive, was completed on 7 December. A data breach notification duty will apply to providers of key infrastructure, such as energy, transport, and finance. The EU Parliament said in a press release that Member States will have to identify concrete "operators of essential services" from these sectors using certain criteria, whether:

- The service is critical for society and the economy,
- It depends on network and information systems, and
- An incident could have significant disruptive effects on its provision or public safety.

Search engines, cloud computing services and online marketplaces, such as Amazon and eBay, will also be affected – they will be required to make sure that their infrastructure is secure, and report major incidents.

EU Member States will be required to set up a network of Computer Security Incidents Response Teams (CSIRTs) to handle incidents. They will discuss cross-border security incidents and identify coordinated responses.

Once published in the Official Journal of the EU, the Member States will have 21 months to transpose the Directive into national law. The final text is not yet available as both the Parliament and the Council will still have to formally adopt the version agreed by the ministers.

- *See http://www.europarl.europa.eu/news/en/news-room/content/20151207IPR06449/html/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity*

Anonymization of personal data in Norway: The DPA's guidelines

The Regulator provides practical guidance for data controllers on what to consider prior to anonymising data. By **Francis A. Medeiros** and **Lee A. Bygrave.**

In August 2015, the Norwegian Data Protection Authority – the Data Inspectorate (Datatilsynet; henceforth 'DI') released a short guidance on the subject of anonymization of personal data, directed at both public and private organizations[1]. In clear language, the guidance describes what anonymization is, what relevance it has to personal data and how it relates to legal compliance. The guidance also explains the difference between anonymization and related concepts, such as pseudonymization and de-identification. Additionally, an annex to the guidance summarizes some anonymization techniques and their respective strengths and weaknesses. The guidance is currently available only in Norwegian.

The guidance

The guidance builds on and in large part replicates the work of the Article 29 Data Protection Working Party (A29WP), particularly the latter's Opinion 05/2014 on anonymization techniques. Thus, it does not add much to the international policy discourse on point; its main utility is to inform Norwegian actors of the benefits, difficulties and legal requirements concerning anonymization.

The chief "selling point" communicated by the guidance is that, by employing anonymization techniques, the processing of data falls outside the scope of data privacy law, as anonymized data is not deemed to be personal data. The DI guides the reader through the definition of personal data according to the main Norwegian data protection legislation: the Act on Processing of Personal Data (2000). The definition therein contains, as the guidance states, three main elements: 1) information in any form that 2) can be related (connected) to 3) an identified or identifiable person. Anonymization, according to the guidance, removes either the "connection" element or the identification of the person to whom the data is related to, making it impossible to relate the information to an individual. Given that anonymized data is not personal data pursuant to the law, a sound motivation for anonymization would be the exemption from compliance with the Act's requirements for the processing of personal data. However, after citing this exemption as a valid reason to anonymize data, the DI emphasises that, to anonymize data, one would already have had to have acquired (and therefore processed) the data, so this advantage is only secondary. One can infer that the guidance proposes anonymization as primarily a valuable tool in respect of the re-use of data.

In its introduction, the guidance sets out some examples of why an organization would want to anonymize "collected" (and therefore already processed) personal data. These could be mainly in situations where there is a need or wish to:

- Publish data
- Release data to a third party while protecting the identity of the data subjects
- Release data for transparency reasons
- Use the data for a new purpose

At the same time, the guidance highlights that even anonymization itself constitutes processing of personal data, and therefore must respect the legal requirements for such processing – for example, purpose specification. The DI states that anonymization could in most cases probably be justified by the legitimate interests of the controller, pursuant to the Norwegian Act § 8f (which transposes Article 7(f) of the EU Data Protection Directive (95/46/EC)).

A distinction between anonymization and pseudonymization is also drawn. The latter is described as a process by which the real identity of the data subject is removed and substituted by a unique designation that later can be reconnected to the subject's identity. This distinction is in line with that made by the A29WP. However, the guidance highlights that some Norwegian legislation operates with a slightly different (and somewhat confusing) conceptual apparatus, relative to the terminology that is common for the EU and other jurisdictions – a point that is important to note for foreign companies. This is particularly the case in the health sector. Thus, Norway's new Personal Health Register Act (2014) has dropped references to pseudonymization and de-identification, operating instead with the category "indirectly identifiable personal health data" (§ 2(b)). This category is defined as data from which names, personal numbers and other person-specific indicators are removed but which can still be reconnected to an individual.

This reconnection risk – referred to in the guidance as "re-identification" – permeates the second part of the guidance, which explains that weak anonymization might reveal or expose personal data whenever the data is cross-analyzed with other data sets containing similar or related information. Following the thrust of the A29WP's Opinion 05/2014, the guidance stresses the difficulties in ensuring that putatively anonymized data cannot be reconnected to separate individuals, and it cites well-known instances of when attempted anonymization failed. It notes that such difficulties are especially acute with respect to genetic data profiles. It further highlights that encryption is not commensurate with anonymization.

In the last part of the guidance, several recommendations are made to those considering anonymization. Again, these recommendations are

taken from Opinion 05/2014. They include the need to undertake the "motivated intruder" test and to regularly revisit the possibility of re-identification in light of changed circumstances. Finally, an annex is attached that sets out strengths and weaknesses of various techniques for anonymization. The material here is taken directly from Opinion 05/2014.

Like Opinion 05/2014, the DI's guidance makes an effort to communicate its subject matter with a minimum of technical jargon. Its intended readership comprises generally organizations that process personal data, not simply technically-savvy personnel. Most, if not all, of the anonymization techniques presented are explained in a denser way in a 2014 report commissioned by the European Union Agency for Network and Information Society (ENISA): Privacy and Data Protection by Design – From Policy to Engineering. The latter report targets regulators and DPAs, and its language is generally less simple than Opinion 05/2014 and the DI's guidance. Nonetheless, it usefully elaborates anonymization (and pseudonymization) techniques within the context of implementing ideals of privacy and data protection by design.

The DI's guidance, however, fails to make salient the close links between these techniques and ideals. This is unfortunate, particularly given the prominence of such ideals in the EU's upcoming Regulation (see Article 23). Thus, the DI has missed a good chance to educate controllers on the future requirements of the Regulation. Of course, the Regulation's final text is still being negotiated, but since Privacy by Design is highly likely to remain an important element of data protection policy discourse for the near future, and since anonymization is one of the major goals of Privacy by Design, it would have made sense to encourage companies to have that in mind when considering anonymization.

AUTHORS

Francis A. Medeiros and Lee A. Bygrave, Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo.

REFERENCES

1 https://www.datatilsynet.no/Sikkerhet-internkontroll/Hvordan-anonymisere-personopplysninger/>.

Privacy dynamics in Latin America

Chantal Bernier takes a look through the prism of the Montevideo seminar of the Ibero-American network of Data Protection Authorities.

Under the aegis of the Spanish Data Protection Authority, the latest seminar of the Ibero-American Network focused on the treatment of personal information in the context of Big Data. The theme is highly topical, not specific to the region, yet the seminar offers a prism on privacy law dynamics in Latin America. Three main streams appear: the vitality of the digital economy in Latin America, the unevenness of privacy regulatory development in the region and the challenge, or opportunity, this development may create for international coherence in privacy law.

Vitality of the Latin American digital economy is buttressed by figures on the information and communications technologies (ICT) market in the region: the 2013 United Nations report on Latin America "Digital economy for structural change and equality" states that the ICT market represents 5.2% of GDP and 8% of the world ICT market, with a growth rate of 12%. Statista reports 327 million Internet users in Latin America with a projected reach of 375 million in 2018.

This vitality was obvious in the seminar with the high level participation of main business actors Hewlett-Packard, Google, MasterCard and Microsoft. Nymity was also well represented as were NGOs and academics. With all the shortcomings that summaries entail, three prominent issues may be said to arise from their insights: the urgency of parameters around the legality of big data analytics to foster innovation in a privacy protective context, the problematic uncertainty around territorial scope of privacy law, illustrated in the current case of Microsoft v. U.S.A. on US law enforcement access to data held by Microsoft in Ireland, and the key importance of integrated corporate governance structures where privacy and data security must be addressed hand in hand.

Economic growth and DP go hand in hand

The high-level of representation, from the public and private sectors, underscored the attention being given to the Latin American evolving privacy regulatory framework.

The unevenness of this evolving regulatory framework is also striking. Mexico has a newly restructured data protection authority which is still reconfiguring its way: all Commissioners are newly appointed and the authority has now been vested with jurisdiction to review findings of subnational data protection authorities. Peru and Colombia data protection authorities are progressing fast, playing catch up with the countries' economic development. Argentina and Uruguay are the only two that have adequacy with Europe. Chile has no data protection authority but a variety of sector specific data protection laws and a push for one, dedicated piece of legislation. Brazil is considering privacy legislation but with its unique balance of privacy and law enforcement access. In addition to Spain, eleven Latin American countries were represented, the rest obviously embarking on the ICT market without a dedicated regulatory framework. The

data protection authorities present particularly raised concerns in relation to the loss of individual control over personal data: consent is undermined by the opacity of data analytics; control becomes illusory in the face of autonomous collection of data through the Internet of Things and through the constant increase of data analytics capacity. Through the discussion, with the concurrence of the private sector, albeit discrete, emerged the resolve to increase verification mechanisms, such as audits and inspections, to ensure compliance in this context of factual disempowerment of users.

The seminar illustrates the imperative and urgent character of capacity building in privacy law in Latin America, which is precisely the purpose of the Ibero-American Network of Data Protection Authorities. This capacity building must be viewed in the general context of democratic and economic growth in Latin America, described in 2012 by the OECD as "solid since 2003 [creating] the possibility for transforming the state, enabling the adoption of ambitious public policies that lock in the prospect of long-term development and mitigate short-term risks". This describes, in my view, the vision through which privacy law development in Latin America must be seen and supported.

Finally, the vibrancy of the Latin American region, with its strong and unique culture, both creates opportunities and poses challenges with respect to global harmonization of privacy law. On the one hand, as the region still develops its privacy legislative frameworks, it is fair to hope it will do so in a coherent manner that contributes to rather than undermines global harmonization of privacy law. On the other hand, it is precisely the strength and uniqueness of Latin America that may hinder that coherence: Latin American countries are choosing the regimes that best suit their legal traditions and socio-economic context, and they are distinct. For example, Uruguay is closer to the European data protection model, while Mexico's legislation has many features in common with Canadian privacy law. Brazil, which has to contend with violence both in the physical and virtual world, requires ISPs to lift the veil of anonymity on the Internet to bring down certain defamatory comments, out of step with the rest of the world which still invokes freedom of expression in that regard with few exceptions, such as in relation to cyber-bullying. Again, this risk of parting ways, albeit in the pursuit of the same goal of protecting privacy, calls for more fora of discussion among States.

DPAs learn from each other

The Ibero-American Network is not the only forum supporting capacity building in relation to domestic privacy protection and fostering international harmonization through regional association. Other fora are key in that regard, bringing together emerging and established data protection regimes: the Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), brings together francophone states, with strong representation from Western Africa; the Common Thread, bringing together Commonwealth member countries includes representation form the Caribbean, Asia and Eastern Africa, with Australia, New Zealand, Canada and the United Kingdom. APEC gathers countries bordering the Pacific also bringing together both established and emerging privacy regimes.

It may be the most striking impression of the Ibero-American Network seminar: in a globalized world, where there can be no privacy protection without a global privacy framework, regional discussions are a key step in that direction.

AUTHOR

Chantal Bernier is Counsel at Dentons LLP, Canada.
Email: chantal.bernier@dentons.com

Facebook and Google release transparency data

Google has released data about the Right to be Forgotten requests it receives. Since end of May 2014, it has evaluated 1,248,260 URLs for removal, and received 352,171 requests. The websites that are most impacted are Facebook.com, profileengine.com. groups.google.com and youtube.com. Google says that the top ten sites account for 9% of all requests.

The pages provide interesting examples of cases. For example, in Italy, Google took the following decision: A high ranking public official asked us to remove recent articles discussing a decades-old criminal conviction. We did not remove the articles from search results.

In the UK, it was decided to remove a news story about a minor crime, and the newspaper published a story about the removal action. "The Information Commissioner's Office ordered us to remove the second story from search results for the individual's name. We removed the page from search results for the individual's name", Google says.

Facebook has issued transparency data about government surveillance in countries around the world.

This report, entitled *Global Government Requests Report*, covers the first half of 2015, and provides information about the number of government requests Facebook receives for data, as well as the number of pieces of content restricted for violating local law in countries around the world where it provides services. The report also includes updated information about the national security requests it received from US authorities under the Foreign Intelligence Surveillance Act and through National Security Letters.

The company says there is an increase in content restrictions and government requests for data globally. The amount of content restricted for violating local law more than doubled over the second half of 2014, to 20,568 pieces of content, up from 9,707. Government requests for account data increased across all countries by 18% over the same period, from 35,051 requests to 41,214.

- *See http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en and http://newsroom.fb.com/news/2015/11/global-government-requests-report-4/*

Hong Kong privacy: Cautious enforcement, strong principles

Although the Privacy Commissioner still has limited powers, the first direct marketing fines have now been issued. By **Graham Greenleaf**.

For seventeen years, Hong Kong's 1995 Personal Data (Privacy) Ordinance, the first comprehensive data privacy law in Asia, remained without substantial amendments. The Amendment Bill of 2012, in force since April 2013, involved fewer changes than were recommended by Hong Kong's Privacy Commissioner, but were nevertheless a significant strengthening of the Ordinance. Two and half years later, the stronger enforcement regime is still only being applied cautiously. However, the Commissioner and the tribunal administering the Ordinance have both given its substantive principles increasingly strong interpretations. This article reviews these developments.

First direct marketing fines issued

Prior to 2012, data users were only required to offer an opt-out at the time of marketing. Post-2012, all data users must obtain prior consent before they make use of personal data for their own marketing uses (Part 6A of the Ordinance), with breaches able to result in a maximum fine of US$64,000. Where data users propose to disclose personal data to third parties for them to use for marketing, there are similar opt-in requirements, and the fact that the personal data is being sold must be disclosed. Fines for breaches can be as high as US$125,000, twice as much as for 'internal' marketing uses. Under both provisions, data subjects must also be informed by the data user, the first time their data is used for direct marketing, that they have the right to opt out from future marketing uses. So there is both a pre-use opt-in and a post-use opt-out.

Until 2015 there had not been any prosecutions under these provisions, but there have now been three in quick succession, in the Magistrates Court. The HK Broadband Network prosecution (Sept 2015) resulted in a fine of HK$30,000 (US$3,850) for a business which ignored a customer's opt-out request, and continued marketing under the pretence of 'end-of-contract' reminders. In the Links International Relocation prosecution (September 2015) a company that acquired another storage company used that company's client details to market its services and was fined HK$10,000 (US$1,300). In the Hong Kong Professional Health Group Limited prosecution (November 2015) there was also a fine of HK$10,000 ($US1,300) for a business' failure to comply with repeated requests to cease marketing communications to an ex-customer of the business.

From 1 April 2013, when the new provisions came into force, until 31 October 2015, the Commissioner has received 535 complaints concerning direct marketing practices, over half of all complaints received. Given that the number of prosecutions is only a very low percentage of complaints received, and the fines are still at a very low level (as they have always been in Hong Kong courts for any privacy-related matters), it has to be questioned whether the prosecutions are having the desired deterrent effect.

Stronger powers of the Privacy Commissioner

Hong Kong's Privacy Commissioner for Personal Data (PCPD) was the first data protection authority created in Asia. A very energetic fourth Commissioner, Allan Chiang, recently completed his five year term. He is succeeded by the fifth Commissioner, Mr Stephen Kai-yi Wong, a former barrister with considerable government and human rights experience, appointed in August 2015. After the 2012 reforms, Hong Kong's Commissioner still has limited powers compared with many DPAs, but they have been made more effective.[1] The Commissioner still cannot issue administrative fines or award compensation.

The Commissioner's principal power is to issue an enforcement notice where he finds a breach of the Ordinance, directing a data user to remedy the breach, and specifying how it should be remedied. Although the legislation is not clear how specific the Commissioner's directions may be, the Administrative Appeals Board in its 2014 decisions concerning *Face Magazine* and *Sudden Weekly* considered it was broad enough to allow the Commissioner to require publishers to issue guidelines to their staff concerning what the Ordinance required in relation to particular types of surveillance.

Before the 2012 amendments compliance notices could only be issued if the breach was likely to be continued or repeated, which enabled data users to simply admit a breach when they were caught out, but face no consequences for repeating the breach. Now, there is no longer any need for a likelihood of continuation before a compliance notice is given, and since failure to comply with a notice is an offence, repeated non-compliance can result in prosecution.

Offences have as yet resulted in only very light fines by courts (as discussed earlier), but in December 2014 a court imposed the first jail sentence (for four weeks) on an insurance agent, for knowingly misleading the Commissioner's office during the course of investigation of a complaint.

Compensation for damage (including mental distress) resulting from a breach of the Ordinance has always been possible (subject to a full defence of taking reasonable care to avoid breach) under section 66 of the Ordinance. However, it has not resulted in a fully litigated claim in nearly twenty years, and nor are

settlements known.[2] The Commissioner cannot award compensation (unlike in Australia), and section 66 claims previously had to go to the Supreme Court, at risk of very high costs orders for unsuccessful claims. Since the 2012 Amendments, they can at least go to the District Court, which does not normally order unsuccessful parties to pay the other side's costs. The Commissioner is now empowered to prescribe forms (none yet prescribed) by which complainants can ask questions of respondent data users. If a data user replies, the reply is admissible and must not mislead, and the court may draw inferences where it is just and equitable to do so from a failure to reply, or an equivocal or evasive reply. The Commissioner can also assist complainants with advice, legal representation and even the negotiation of 'compromises', with the Commissioner's costs of legal representation as a charge against any compensation awarded. Application forms and other assistance are available from the PCPD website.[3] At least one application has been accepted, and four more were recently still pending, but there are no known cases which have been heard, or have resulted in settlements.

The Commissioner can also assist complainants with advice, legal representation and even the negotiation of 'compromises'...

The Commissioner has also continued to name the respondents in significant complaints that he chooses to report under section 48(2) of the Ordinance ('Investigation Reports'), a conscious 'name and shame' policy introduced by the previous Commissioner to help compensate for his otherwise limited powers. He has done so on thirteen occasions since 2013,[4] including in the examples following.

Strength of HK's Principles continue to surprise

In three areas of substantive privacy law, Hong Kong's data protection principles (DPPs) have been strengthened by recent decisions of the Commissioner and the Tribunal: publicly available information; 'unfair' means of collection; and collection limitations.

'Publicly available information' is still 'personal data'

Hong Kong does not have any general exemption from its use limitation principle (DPP 3) for 'publicly available information'. DPP may therefore apply to the use of personal data collected from sources such as public registries or web sites. The Commissioner held in 2013 in the 'Do No Evil' Investigation Report[5] that a database accessed through a smartphone app that was built from the aggregation of personal data from numerous government registries and websites was in breach of DPP 3. A key aspect of the Commissioner's finding was that the relevant purpose of collection for DPP 3 was the purpose (express or implied) of the government agency when it originally collected or created the data, not the purpose of the company when it collected the data to create the database.[6] It seems that all public registers in Hong Kong may have some implied limits on the use of personal data they contain. It was a controversial decision, but there was no appeal against it to the Administrative Appeals Board (AAB).

In October 2015 the AAB ruled on an appeal against the Commissioner in the Webb-site decision,[7] a case with different facts but which raised many similar arguments. Webb-site provides information about people involved in public and statutory offices, directors of listed companies, and holders of certain licences in Hong Kong. 'X', a female member of various statutory panels had also been involved in matrimonial proceedings. Decisions in three judgments were included in the Judiciary's website, initially identifying the parties, but subsequently anonymised by the court at the request of X. However, on Webb-site, under X's name there were hypertext links to the three judgments, effectively identifying X as the female party in those proceedings. A search for X's name on Webb-site would produce this information. X complained to the Commissioner, who issued an enforcement notice requiring removal of the hyperlinks.

In a complex decision which requires more analysis than is possible here, the AAB made a number of key findings, including that i) DPP 3 does apply to publicly available information; ii) that the purpose of the judiciary in collecting and using the personal data was 'to enable their judgments to be utilized as "legal precedents on points of law, practice and procedure of the courts and of the public interest"; iii) the purpose of Webb-site's use of the data was 'reporting and publication for general use' and was not 'in any way related to the law', and was therefore in contravention of DPP 3; and iv) the Commissioner's decision was reasonable that the disclosure of X's identity did not promote transparency or other important public interests, and the removal of the hypertext links did not conflict with the freedom of speech and expression guarantees in Hong Kong's Basic Law and Bill of Rights Ordinance (BORO). There is no appeal from AAB decisions to the Courts, only the possibility of judicial review. Surprisingly, the AAB decision did not involve any discussion of possible differences between republishing personal data (as in the 'Do No Evil' case) and providing hypertext links and associated data enabling identification of the subjects of publicly available data (as in this case). Hong Kong now has in some cases a 'right to remain anonymous' which shares some similarities with the 'Right to be Forgotten' developed under European law, at least insofar as both involve removal of hypertext links. The PCPD's office has confirmed that its stance is not 'to ask for removal of articles from the archives of newspapers and publishers but only, as in this case, to seek removal of links in some cases.[8]

Collection by 'unfair' means

Data Protection Principle 1 (DPP 1) requires collection which is 'fair in all the circumstances of the case'. In previous decisions in 2012 concerning the publications *Sudden Weekly* and *Face Magazine* the Commissioner applied DPP 1 to intrusive media practices involving long distance photography of intimate activities, by photography into celebrities' homes from adjoining hillsides. He found that these practices were 'unfair' under DPP 3. The Commissioner's decisions were upheld by the Administrative Appeals Board (AAB).[9] As a result public figures have some privacy rights in Hong Kong with similarities to the position under European law.

In the 'Blind' 'recruitment' advertisements decision in 2015[10] the Commissioner found that employment advertisements that do not identify either employer or agency are unfair collection, because they could be collecting personal data for purposes other than employment consideration, including fraudulent purposes. He named the employment agencies involved in such practices, about which he had previously warned, and stated that he had served 42 more enforcement notices on the parties concerned. As discussed above, continuation of the practice will now expose those agencies to potential offences.

Limitations on 'excessive' collection

DPP 1 limits the collection of personal data to that which is necessary for a lawful purpose directly related to a function of the collection, and not excessive in relation to that purpose. In the Queenix decision[11] the Commissioner found that the practice of a fashion house to fingerprint its employees was excessive collection which ignored less intrusive alternatives which would have been sufficient for both security and attendance purposes. He also found it was unfair collection, as consent by employees to the practice was neither genuine nor informed. The Ordinance does not have separate protections for 'sensitive' data, but examples such as this indicate that collection of data such as fingerprints requires a higher level of justification. Other Investigation Reports in 2015 have involved excessive collection of personal data though mobile apps and membership programs in the travel industry, and of private tutors through tutorial agency websites.[12]

More data subject rights through contracts

Until this year, Hong Kong adhered quite strictly to the doctrine of privity of contract, which provides that non-parties cannot enforce provisions in contracts between other parties. This prevented data subject from enforcing provisions in contracts between data users and contracted data processors (whether or not located in Hong Kong), even when these provisions were clearly intended to protect data subjects against wrongful actions by processors.

The Contracts (Rights of Third Parties) Ordinance 2014, which came into force in 2015, allows third party enforcement, but requires the contract terms purporting to benefit third parties identify them individually or as a class, and that the contract must not exclude enforceability either expressly or impliedly. This may make it easier for Hong Kong to implement data export mechanisms that require data subjects to have enforceable rights (e.g Binding Corporate Rules).

REFERENCES

1 For more details, see G Greenleaf Asian Data Privacy Laws: Trade and Human Rights Perspectives (OUP, 2014), pgs 109-116.
2 There was a newspaper report of one award of HK$5,000, but there was no written decision.
3 PCPD 'Legal Assistance' <https://www.pcpd.org.hk/english/legal_assistance/assistance.html>
4 HKPCPD 'Investigation Reports' <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/invest_report.html>
5 Glorious Destiny Investments Limited and Brilliant United Investments Limited Publicly Disclosed Litigation and Bankruptcy Information Collected from the Public Domain to Their Customers via Smartphone Application "Do No Evil" (2013) HKPCPD s48(2) report R13–9744, 13 August 2013 <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_9744_e.pdf
6 Greenleaf, G 'Private Sector Uses of 'Public Domain' Personal Data in Asia: What's Public May Still Be Private', Feb 2014, *Privacy Laws & Business International* Report, 13-15.
7 David M Webb and Privacy Commissioner for Personal Data (2015) Administrative Appeals Board, 27 October 2015 <www.pcpd.org.hk/english/files/casenotes/AAB_54_2014.pdf>
8 PCPD Media statement 'PCPD Welcomes Administrative Appeals Board's Decision on Dismissing David Webb's Appeal Case' 29 October 2015 https://www.pcpd.org.hk/english/news_events/media_statements/press_20151029.html>
9 See Greenleaf Asian Data Privacy Laws, pgs. 94-95 for discussion.
10 Unfair collection of personal data by the use of "blind" recruitment advertisements (2015) HKPCPD s48(2) Report R15–8107, 21 July 2015 <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R15_8107_e.pdf
11 Collection of Fingerprint Data by Queenix (Asia) Limited (2015) HKPCPD s48(2) Report R15-2308, 21 July 2015 <https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R15_2308_e.pdf
12 For details, see HKPCPD 'Investigation Reports' at the address cited above.

What is to be done with the e-Privacy Directive?

The EU Commission could propose a further Regulation in this area – in any case, a solution is needed, say **Francis Aldhouse** and **Liz Upton**.

As well as the current wide sweeping reforms being proposed to the existing European data protection framework (and in particular the introduction of a new Regulation[1] to replace the Data Protection Directive[2]), another area which will need reviewing in the near future is the regulation of the electronic communications sector and the e-Privacy Directive[3].

The e-Privacy Directive which forms part of the Regulatory Framework for Electronic Communications was first adopted in 2002 and, amongst other things, specifies how some of the principles in the Data Protection Directive apply to the electronic communications sector. The e-Privacy Directive was further amended in 2009[4] as part of a package updating the Regulatory Framework and by January 2013, all Member States had notified the necessary measures to implement the e-Privacy Directive into their national laws.

The European Commission has recognised in its proposal to reform the existing data protection framework that changes will be needed to reconcile the application of this new Regulation with the e-Privacy Directive. Indeed, the proposed Regulation makes a limited number of technical adjustments to the e-Privacy Directive to take account of the fact that the Data Protection Directive is being transformed into a Regulation and the Commission has undertaken to carry out a further review in this area once the Regulation has been published.

In order to prepare for this review, the Commission asked a team of consultants to undertake a study of the transposition and effectiveness of the specifically privacy related articles of the e-Privacy Directive, and also to consider the relationship of the e-Privacy Directive to the proposed Regulation. The outcome of the study was published as a report in June 2015[5] (the 'Report') and raises interesting questions for the fate of the e-Privacy Directive. It is a lengthy document (122 pages) with additional detailed supporting material in the Annexes. This article seeks to summarise the scope of the Report, focussing particularly on the consultants' recommendations for legislative changes.

The Report

The Report does not deal with the entire e-Privacy Directive but looks in detail at the following five specific topics, providing evidence of how they have been implemented and enforced in practice, suggesting gaps and potential areas for change and examining how the Directive should operate with the Regulation:

- Scope of the e-Privacy Directive (Articles 1 to 3)
- Confidentiality of communications (Article 5(1))
- Cookies, spyware and similar techniques (Article 5(3))
- Traffic and location data (Article 6 and 9)
- Unsolicited commercial communications (Article 13).

Scope of the e-Privacy Directive (Articles 1-3)

The provisions of the e-Privacy Directive are applicable to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices".[6]

The Report takes a detailed look at the definitions which make up this statement which highlights how complex it can be to work out whether the e-Privacy Directive is applicable to particular services and also how it can result in artificial distinctions being drawn where services that are very similar from a functional perspective are in fact regulated by different legal regimes. For instance, broadcasting services which are intended for a potentially unlimited audience are not covered (eg. near video on demand services NVOD) but when the individual subscriber or user who is receiving that information that is part of the broadcasting service can be identified, then it will be covered (eg. video on demand services). Information society services are also excluded from the definition of "electronic communications services" and yet certain provisions in the e-Privacy Directive such as those dealing with cookies are almost certainly applicable to such services. This confusion is further compounded by the fact that the e-Privacy Directive has also not been transposed into the national legislation of the Member States on a consistent basis, with certain provisions being transposed into legislation dealing with general data protection laws or other laws dealing with information society services or consumer protection. This means that different services can therefore be treated differently in each Member State.

The Report goes on to note that in contrast to the Data Protection Directive there are no applicable law provisions in the e-Privacy Directive. In the authors' view, which is perhaps controversial, in the absence of such an explicit provision, the same principles should currently be applied as to the rest of the European Regulatory Framework for Electronic Communications, namely the place where the services are provided and they conclude that the applicable laws rules in the Data Protection Directive (which look to where the operator is established) would not be applicable to the e-Privacy Directive.

In the authors' view, given growing convergence and technological developments, it no longer makes sense to distinguish technologically between information technology services, telecommunications services and media services. Indeed, they have the greatest doubts about whether the regulation of these activities in three separate sectors is sustainable. However, they highlight that this is an issue which goes beyond

the e-Privacy Directive because it is a distinction which is underpinning all European regulation dealing with the online environment. As such, it is unlikely to change in the short term, so the Report therefore recommends instead, looking at what changes can be made to the existing e-Privacy Directive to help ensure consistency.

Recommendation

The recommendation is to amend Article 3 of the e-Privacy Directive to 'make its provisions applicable to the protection of privacy and the processing of personal data "in connection with the provision of publicly available services in public or publicly accessible private communications networks in the Union".' The Report suggests that this amendment "would put an end to the discussion about the applicability of the provisions of the ePrivacy Directive to information society services and other value-added services provided via public electronic communications networks.' and "remedy the currently perceived distortion in which very similar services are subject to different regimes and the consequent uneven playing field".

Confidentiality of communications (Article 5.1)

The Report next turns to the duties in Article 5.1 to keep communications confidential. This Article states that: "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services through national legislation" and that "in particular, [the member states] shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users".

The Report notes that Member States have all had legislation for many years protecting the confidentiality of private communications (together with national exemptions for security and criminal investigation purposes) and that therefore the transposition of Article 5.1 did not have a harmonising effect in this regard. Nor do the consultants believe that this will change with the new draft Law Enforcement Directive[7]. These elements are so deeply integrated in matters within the jurisdiction of Member States that harmonisation is unrealistic. Nevertheless, the consultants propose changes to reflect their general approach of widening the scope of the e-Privacy Directive beyond public electronic communications systems.

Recommendation

Consistent with the proposed changes to Article 3 the Report suggests making the provision applicable to "confidentiality of communications and the related use of traffic data by means of a public or publicly accessible private communications network".

Secondly, in the authors' view, it is uncertain what the current drafting of this provision means for technologies which are fully automated and which register electronic communications (such as deep packet inspection systems used to detect malware or mobile apps which access contact lists or SIM card data). The Report questions whether such intrusions are justified and that even with the consent of the user under Article 5.3 whether they are incompatible with the proportionality principle applicable to the processing of personal data. The Report concludes that a recital should be added which clarifies that the confidentiality of electronic communications should be protected against "automatic" intrusions without human intervention.

Thirdly, the exception in Art. 5.2 for "technical storage which is necessary for the conveyance of a communication" should probably be broadened to "storage as far as necessary for ensuring the functioning of the network or the provision of the service on that network". This is consistent with the Report's proposed extension of scope of Article 5.1 to information society services.

Finally in this chapter, the Report considers in some detail the lawful business exemption in Article 5.2. This states that the protection of confidentiality "shall not affect any legally authorised recording of a communication and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication".

Again this exemption has been transposed by Member States in very different ways: The United Kingdom and Belgium are notable for their extensive use of the exemption, but some Member States have made no such provision at all seemingly because it is thought to be too prejudicial to general rights to the privacy of communications. The consultants suggest that the scope of this exemption be clarified to allow further harmonisation in this area. They propose widening it to other situations such as the recording of communications in an employment context for quality control or legitimate supervision of work performance. However, a careful assessment of the impact of such change on stakeholders would be needed to assess its feasibility, taking into account the diversity of rules currently applicable to the processing of personal data in the employment context.

AUTHORS

Francis Aldhouse, Consultant and Liz Upton, Senior Associate, Bird & Bird.
Emails: francis.aldhouse@twobirds.com, elizabeth.upton@twobirds.com

REFERENCES

1 Commission's Proposal for a Regulation on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
4 The e-Privacy Directive was amended in 2009 by the Citizen's Rights Directive 2009/136/EC.
5 http://ec.europa.eu/digital-agenda/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data
6 Article 3 e-Privacy Directive (as amended).
7 Draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

INFORMATION

The second part of this article: http://www.twobirds.com/en/news/articles/2015/global/what-is-to-be-done-with-the-e-privacy-directive-part-2

Korea amends its DP Act and legislates on cloud computing

Cloud computing service providers subject to data breach notification rules and all data controllers to stronger provisions on liability. By **Kwang Bae Park**.

In 2011, South Korea enacted the Personal Information Protection Act (PIPA) which broadly regulates the collection and handling of any personal information by a data handler.[1] PIPA combined elements of previous legislation, the "Public Institutions Act"[2] and the "Network Act",[3] to become a comprehensive act covering both the public and private sectors. The Network Act continues to regulate the processing of personal information in the context of services provided by information and communications service providers (ICSPs). Other sector specific laws complement PIPA[4] and will generally take precedence over PIPA whenever applicable. Otherwise, PIPA would apply to any entity or individual that handled personal information. The basic regulatory schemes for the protection of personal information under the PIPA and the Network Act (and for most purposes the Credit Information Act) are substantially similar to each other.[5] This article will explain the key regulatory reforms to Korea's data protection and privacy laws since 2012 which have cumulatively established one of the strictest regulatory regimes in the world.

I. 2012 Comprehensive Plan for Minimizing Collection and Use of Resident Registration Numbers

With the rapid development of the Internet in Korea, Resident Registration Numbers (RRNs) became extensively used for online identification purposes when registering an account with most Korean websites. However, this practice of using RRNs for online identification received heavy criticism after persistent security breaches resulted in the repeated leakage of large amounts of users' personal information including their RRNs. In response, the Korea Communications Commission (KCC), the Ministry of Public Administration and Security, and the Financial Services Commission jointly announced a "Comprehensive Plan for Minimizing Collection and Use of Resident Registration Numbers" in April 2012. The regulators' main objective was to sharply limit the collection and use of resident registration numbers (RRNs) in both the public and private sectors. As a result, the Network Act[6] and PIPA were both amended to include provisions prohibiting the collection and use of RRNs unless falling under certain limited exceptions.

2012 Amendment to the Network Act

The Network Act was amended in February 2012, which among other changes, placed restrictions on the collection and use of resident registration numbers (RRNs) and introduced measures to improve the overall level of data protection in Korea. Under the amendment, ICSPs were no longer allowed to collect or use RRNs of their service users unless certain limited exceptions applied and were required to dispose of all previously collected RNNs within two years from the effective date of the amendment. In addition, ICSPs became obligated to: (i) immediately notify users and the KCC of any data leaks or breaches and implement measures to minimize the damage to users; (ii) dispose of personal information unused for a certain period of time; (iii) regularly notify users on the details of the personal information collected and used; and (iv) obtain Information Security Management System (ISMS) certification if they met certain criteria.

2013 Amendment to the PIPA

The PIPA was amended in August 2013 and introduced measures that prohibited the collection and use of RRNs, irrespective of consent, unless expressly allowed by other statutes or deemed necessary in emergency situations. A violation could result in a fine of up to KRW 30 million (£17,000). Furthermore, a maximum fine of KRW 500 million (£284,000) could now be imposed on a data handler that failed to protect RRNs. This fine could only be waived if the data handler successfully proved that all prescribed measures necessary for securing the safety of personal information had been implemented. Finally, all previously collected RNNs would have to be disposed of within two years from the effective date of the amendment.

II. 2014 Comprehensive Solution Package for Enhanced Data Protection

In response to massive data breaches at three major South Korean credit card companies in January 2014, public sentiment again swung decisively toward increased regulation of the processing of personal information. In July 2014, a cross-government task force of 18 government agencies recommended a comprehensive solution package (the CSP) with 98 subcategories designed to strengthen the PIPA, Network Act[7], Credit Information Act and other sector specific laws. Specifically, the CSP aimed to gradually amend Korea's data protection and privacy laws to: (i) allow punitive and statutory damages for certain violations; (ii) create the position of Chief Protection Officer (CPO) and increase the potential liability of corporate officers and directors; (iii) allow greater flexibility to companies to design technical and managerial safeguards; (iv) allow individuals to change their RNNs in limited cases and strengthen regulations for minimizing the collection and use of RRNs; (v) clarify the scope of entities and persons subject to the PIPA, Network Act, and Credit Information Act, respectively.

2014 Amendment to the Network Act
The Network Act was amended in May 2014 and ICSPs became obligated to: (i) collect only the minimum level of personal data that is necessary for service provision, irrespective of consent; (ii) report data breaches within 24 hours to the relevant authority (KCC or KISA); (iii) ensure that personal information requiring destruction (because the retention period expired or the purpose for which the data was used was completed) could not be restored or reconstructed and a criminal penalty provision was introduced for related violations; (iv) pay statutory damages of up to KRW 3 million (£1,725) to each affected user for a negligent or willful violation of a data protection requirement that causes data loss, theft, or leakage without the user having to prove actual damage resulting from such violation; (v) pay increased administrative fines of up to 3% (previously 1%) of the ICSP's annual turnover for failure to obtain user consent prior to the collection and use of personal information, and the cap of KRW 100 million (£57,480) for administrative fines previously applicable to data leaks resulting from failure to comply with technical and managerial protection measures was removed; (vi) appoint a Chief Information Security Officer (CISO) if they met certain criteria; and (vii) obtain the user's opt-in consent prior to transmission of direct marketing materials by electronic means.

2014 Amendment to Standards of Personal Information Security Measures
In December 2014, the Ministry of Government Administration and Home Affairs (the MOGAHA[8]) amended the "Standards of Personal Information Security Measures" (the Standards). The Standards were issued by the MOGAHA as a guidance notice under the PIPA and set forth specific data security requirements that data handlers are obligated to comply with when processing personal information. The amended Standards included new measures: (i) to increase oversight of third-party service providers when outsourcing personal information; (ii) to control use of mobile devices and auxiliary storage devices (eg. USB flash drives); (iii) to increase obligations to review access logs; (iv) to impose more detailed standards for destruction of data (as required by expiry of retention period or completion of purpose for which the data is used); (v) for a stricter user authentication process for data handlers authorized to collect and use RRNs under the PIPA; and (vi) requiring data handlers that process particular identification data (PID) to conduct a vulnerability assessment at least once a year to prevent PID from being leaked, falsified, or damaged through their internet websites.

2015 Amendment to the Credit Information Act
The Credit Information Act was amended in March of 2015 with the aim of increasing the overall level of regulatory requirements applicable to the protection of personal credit information of individuals. The key amendments were: (i) the requirement to appoint Credit Information Custodians/Managers' who were obligated to report regularly to the CEO and the Board, and also provide reports to the Financial Services Commission (the FSC), and representative directors (eg. CEOs) were required to directly oversee the company's credit information security status; (ii) stricter regulations (eg. encryption of personally identifiable information, education of outsourced provider on the secure management of credit information, etc.) when outsourcing the processing of credit information; (iii) the requirement that separate, individual consent from the data subject is needed in order to disclose the data subject's personal credit information to a third party or for a credit bureau company or public credit registry to be provided with the data subject's personal credit information; (iv) the requirement that consent for information which is necessary for the transaction and for information which is optional, must be unbundled and obtained separately, and service cannot be refused because of failure to obtain optional consents; (v) the requirement to limit the retaining period for personal credit information to 5 years after completion of a transaction and that data on completed transactions (dormant data) be handled separately; (vi) administrative penalties of up to 3% of the relevant business' annual revenue for disclosure for non-business purposes of confidential data, or knowing use of illegally disclosed data and up to KRW 5 billion (£2,875,000) where failure to establish a security plan results in personal credit information being lost, stolen, leaked, fabricated, or damaged; (vii) punitive damages of up to 3 times the damage caused by personal credit information being lost, stolen, leaked, fabricated, or damaged due to the relevant business' willful misconduct or gross negligence; and (viii) statutory damages of up to KRW 3 million (£1,725) per data subject whose personal credit information was stolen, lost, leaked, fabricated, or damaged due to the relevant business' willful misconduct or negligence.

2015 Amendment to Standards of Technical and Managerial Measures for the Protection of Personal Information
In May 2015, the KCC amended the Standards of Technical and Managerial Measures for the Protection of Personal Information (the Network Standards). The Network Standards were issued by the KCC as a guidance notice under the Network Act and set forth specific standards for the technical and managerial measures required for ICSPs to protect users' personal information. The most significant change in the amended Network Standards is that they have now become minimum requirements for ICSPs, who may still be required to implement additional information protection measures depending on the size of their business and the volume of personal information collected. Prior to the amendment, even if personal information was stolen or leaked from ICSPs by third parties (eg. by hacking), ICSPs were generally not found to be in violation of the Network Act if they had adopted protection measures in accordance with the specific standards set forth in the Network Standards. Many ICSPs that experienced hacking and leakage of their users' personal information, successfully defended the users' claims for damages using the argument that they fully complied with the Network

Standards. However, after the amendment of the Network Standards, such arguments will be less prevalent because the prescribed measures are now only the minimum measures to be taken by ICSPs. Also, the amended Network Standards requires ICSPs to store personal information such as RRNs, passport numbers, driver's license numbers, alien registration numbers, credit card numbers, bank account information, and bio information in encrypted form through the use of secure encryption technology.

2015 Amendment to the PIPA

The PIPA was most recently amended in July of 2015. Among other changes, it increased the potential liabilities of data handlers. Under the amendment, the court may order a data handler to pay an amount up to 3 times the actual damages of the data subject if the data subject can prove: (i) an intentional or grossly-negligent violation of the PIPA by the handler; (ii) that the data subject's personal information was lost, stolen, leaked, forged, falsified or damaged due to such violation; and (iii) the actual amount of damages resulting from such a violation. The amendment also added a statutory damages provision that allows a data subject to claim up to KRW 3 million (£1,725) in damages when the data subject can prove (i) willful misconduct or negligence of the handler, and (ii) the fact that data subject's personal information was lost, stolen, leaked, forged, falsified or damaged because of the willful misconduct or negligence. Like the statutory damage provisions under the previously amended Network Act and Credit Information Act, this new statutory damage provision under the PIPA applies even if the data subject is unable to prove the actual amount of damage caused by the violation of the PIPA by the data handler. Finally, the amendment awards broader authority to the Personal Information Protection Commission (PIPC) to (i) recommend improvements of policies and systems, (ii) conduct an inspection to assess whether the recommendations are being implemented properly, (iii) request the submission of materials and (iv) appoint or commission mediators to the Personal Information Dispute Mediation Committee. The new provisions under the PIPA will become effective on July 25, 2016.

III. The Act on the Development of Cloud Computing and Protection of Users

The Act on the Development of Cloud Computing and Protection of Users (the Cloud Computing Act), came into effect in September of 2015, six months after promulgation. The Cloud Computing Act was designed to provide a framework for promoting the use of cloud computing while also aiming to protect the users' cloud services data. Companies that use cloud services provided by another company are eligible to obtain business licenses and permits required under other laws, because they will be deemed to be equipped with the computing facilities stipulated by such laws, even if they do not have their own computing facilities. However, this provision will not apply in certain cases, such as where the subject law prohibits the use of cloud computing. The Cloud Computing Act also stipulates that, fundamentally, the PIPA and Network Act will apply to the protection of user data stored on clouds (Cloud Data) but it also includes separate provisions on the protection of such Cloud Data. Specifically, cloud computing service providers (CCSPs) are required to notify users of any cyber security incidents, data leakages, and service interruptions, and also notify the Minister of Science, ICT & Future Planning (SIP) in the event Cloud Data is leaked. Users may also demand from the CCSP the names of any countries in which their Cloud Data is stored, and, if the Minister of SIP determines that such disclosure is necessary for user protection, he may recommend that the CCSP provide the said country information to its users. Finally, the provision of Cloud Data to third parties by CCSPs is also strictly limited, and, upon expiration of the service agreement between the CCSP and the user or the termination of cloud services, the CCSP is obligated to return the user's Cloud Data to the user or destroy such data if returning it is impossible.

IV. Development of Certification Systems

As previously mentioned, the 2012 amendment to the Network Act obligated ICSPs to obtain ISMS certification if they met certain criteria. By contrast, the following certifications are not legally mandatory. They are operated based on voluntary participation by subject entities.

Personal Information Management System

The Personal Information Management System (PIMS) was created by the 2012 amendment to the Network Act and further rules governing the certification process were subsequently prescribed through a guidance notice issued by the KCC in 2013. The certification process will mainly assess: whether an applicant is protecting personal information in a periodic and systematic manner; whether the required managerial, physical, and technical measures are being implemented for the protection of personal information; and regulation compliance throughout the life-cycle (collection, use, and destruction) of personal information. The KCC will consider up to a 50% deduction for PIMS certified ICSPs when determining the penalty surcharges / administrative fines for a violation under the Network Act.

Privacy Information Protection Level

The Privacy Information Protection Level (PIPL) certification system was created in October of 2013 by a guidance notice issued by the Ministry of Security and Public Administration (MOSPA) pursuant to the provisions of the PIPA. The PIPL certification system was designed to encourage companies' voluntary compliance with the safeguard requirements of the PIPA for data protection. Upon certification, companies and government agencies became eligible for reduced supervision and potentially reduced penalties. The 2015 amendment to the PIPA provided a statutory basis for using the PIPL certification system as a legitimate means for determining whether the safeguards and measures taken with regard to personal information processing are in compliance with

PIPA and for marking and advertising the substance of the PIPL certification obtained.

Outlook

With the rapid advance of its IT, Korea's data protection laws have remained in a constant state of flux. Following the creation of the PIPA in 2011, a series of amendments have been enacted in response to various violations including several incidents of mass data leakage. As a result, data handlers and their outsourced data processors have become subject to strict regulations and their accountability to data subjects has increased considerably. Recently, there has been increased discussion on the need to achieve a more appropriate balance between the protection of personal information and its commercial utilization. It remains to be seen whether such discussions will lead to more practical legislative or regulatory changes in the near future.

AUTHOR

Kwang Bae Park, Partner and head of the Data Protection & Privacy Practices, Lee & Ko, Seoul.
Email: kwangbae.park@leeko.com

REFERENCES

1 A public agency, company, organization, or individual that by itself or through a third party, handles 'personal data' to make use of or carry out any operation of a 'personal data file' in the course of or in relation to its business activities. A concept similar to 'data controller' under the EU Directive No. 95/46/EC.
2 Act on the Protection of Personal Information Maintained by Public Institutions.
3 Act on Promotion of Information Communication Network Usage and Information Protection.
4 These include the Act on the Use and Protection of Credit Information (the Credit Information Act), the Electronic Financial Transaction Act, the Act on the Use and Protection of Location Information, etc.
5 These regulatory schemes include: 1) notice and consent requirements for the processing of personal information; 2) technical and managerial protection measures that are required to be taken by data handlers/ICSPs; 3) disclosure of privacy policies and appointment of privacy officers; 4) the right of data subjects; and 5) the data handler/ ICSP's obligations related to data leakage, such as reporting obligations to government agencies and payment of damages to data subjects. The regulatory scheme for the protection of personal credit information under the Credit Information Act is also similar to those under the PIPA and the Network Act but also retains important differences due to sector specific characteristics.
6 Actually amended in February 2012, preceding the Comprehensive Plan for Minimizing Collection and Use of RRNs.
7 Actually amended in May 2014, preceding the CSP.
8 Became the Ministry of the Interior (MOI) in September 2015.

Facebook... from p.3

the views of the various courts on the matter of jurisdiction have been mixed. The ruling in the so-called "Google Spain" case has led to further assertions by a number of European data protection authorities that they have jurisdiction and that their national laws apply to Facebook's processing of data of citizens of those countries. Ultimately, … the Courts … will decide these questions. It is clear that the 1995 EU Data Protection Directive did not ring-fence the concept of a "main establishment" in law as is envisaged under the General Data Protection Regulation which has led to varying interpretations of jurisdiction and applicable law in a number of cases'.

DPAs united?

In 2014, following Facebook's global revision of its data policy, cookie policy and terms, the DPAs of the Netherlands, France, Spain, Hamburg and Belgium formed a European level contact group. On 4 December, they issued a statement regarding this case, as well as the recommendations of the Belgian Data Protection Authority[5]. They say that while they recognise the right of Facebook to appeal the tribunal's judgment, the contact group expects Facebook to comply with these orders in all territories of the EU as a means of contributing to ensure consistency with the requirements of the European DP Directive and the Privacy and Electronic Communications Directive.

"This statement is without prejudice to the ongoing national investigations and to measures that could consequently be imposed upon Facebook. The measures adopted by Facebook should not bring undue prejudice to the Internet user," the DPAs say. PL&B expects that the contact group will ask for support from the other EU Member States' DP Authorities.

INFORMATION

The Brussels-based lawyers representing the Belgian DPA were Frederic Debusseré, Partner; Jos Dumortier, Partner; and Ruben Roex, Associate; from the law firm, time.lex. The Brussels-based lawyers representing Facebook Belgium were Dirk Lindemans, Partner, Liedekerke Wolters Waelbroeck Kirkpatrick; and Henriette Tielemans, Partner, Covington & Burling.

REFERENCES

1 The Tribunal's judgement in English: https://www.privacycommission.be/sites/privacycommission/files/documents/Judgement%20Belgian%20Privacy%20Commission%20v.%20Facebook%20-%2009-11-2015.pdf
2 The full text of the Belgian Privacy Commission's order is at https://www.privacycommission.be/en/news/judgment-facebook-case
3 For background, see http://www.privacycommission.be/en/news/13-may-belgian-privacy-commission-adopted-first-recommendation-principle-facebook
4 The academic study From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms: http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf
5 Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg & Belgium: https://www.privacycommission.be/en/search/site/Common%20Statement%20by%20the%20Contact%20Group%20of%20the%20Data%20Protection%20Authorities

Strong reactions to invalidation of Safe Harbor

Whilst the majority of DPAs have a wait-and-see policy until January 2016 on the question of EU-US data transfers, some have taken action. Israel has virtually banned transfers based on the Safe Harbor regime, saying that it has revoked its earlier authorizations.

In Germany, there has been a heated debate and some Land (state) DPAs have announced that they will immediately start to look into data transfers from the EU to the US by Facebook, Google, and others, and may stop data flows. The Hamburg Commissioner has specifically said that companies which transfer data to the US exclusively based on the Safe Harbor decision, act unlawfully. From February 2016, these companies must reckon with measures taken by the supervisory authorities, it says. The Hessen DPA says it will in general not take any retroactive enforcement action on Safe-Harbor based transfers if the transfer tools were used in good faith. "In this way, we avoid the "ex tunc" [from the beginning] and "ex nunc" [from now] issue.

Also the Dubai International Financial Centre (DIFC) in Dubai says that transfers to US cannot rely on Safe Harbor, reports law firm Latham and Watkins. The DIFC Commissioner for Data Protection has issued guidance on the adequacy of the US Safe Harbor.

Dubai's law (Article 12) does not expressly envisage the use of EU-style model clauses or binding corporate rules. The Commissioner has previously issued guidance that it will take use of model clauses or binding corporate rules into account as evidence that an organisation is applying adequate safeguards where an organisation applies for a permit to transfer under Article 12(1)(a). Failure to comply with Articles 11 and 12 of the DIFC Data Protection Law may result in a claim for compensation by a data subject at the DIFC Courts, an inspection by the Commissioner and issue of direction requiring compliance and the imposition of a financial penalty by the Commissioner for non-compliance. Given the potential for financial penalties and the absence of a grace period for compliance with the guidance, we would suggest that organisations urgently review the basis upon which they transfer personal data from the DIFC to the US to ensure that they continue to remain compliant, Latham and Watkins' lawyers say.

The US Department of Commerce published an advisory on the Safe Harbor website stating: "In the current rapidly changing environment, the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework".

After these initial reactions, the EU Commission issued guidance on EU-US transfers advising on the alternative methods than can be used, such as model contracts or Binding Corporate Rules.

- For Israel, see https://iapp.org/media/pdf/resource_center/ILITA_SH_Statement.pdf
- For Dubai, see http://www.globalprivacyblog.com/privacy/difc-in-dubai-says-transfer-to-us-cannot-rely-on-safe-harbor/
- For Hamburg, see https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Information_on_the_Safe_Harbor_ruling_of_the_Court_of_Justice.pdf
- The European Commission's communication is at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

Netherlands: Nike alters running app after DPA investigation

Nike has made modifications to its running app following an investigation by the Netherlands Data Protection Authority. The DPA said that Nike+ Running app provided insufficient information about the processing of the users health data. Nike has now agreed to several modifications; new users of the app are no longer obliged to give their height and weight. New versions of the app also contain extra information about the processing of height and weight data. Nike has announced further measures for better informing all users about the processing of their health data in the coming months. It has also announced that it will belatedly seek consent from all existing users to the processing of their health data, the DPA informs. The Dutch DPA will now evaluate whether the action taken is enough to make the app compliant with data protection law.

The app can track distance, speed, time and number of calories burned. Users can use personal training programmes via the app to improve their performance. For these programmes, the app uses the GPS and network-based location data from the phone and the acceleration sensor (accelerometer). As the device monitors performance, it also generates health data which should be treated as sensitive data.

The DPA said that Nike does not inform individuals well enough about the types of processing which are:

1. The tracking (on Nike's servers) of (developments in) the sporting performance of the individual
2. Comparison of the individual's sporting performance against the average of a comparable group of people.
3. Research and analysis purposes.

- *See https://www.cbpweb.nl/en/news/translation-press-release-10-november-2015-nike-modifies-running-app-after-dutch-dpa and conclusions of the investigation at https://cbpweb.nl/sites/default/files/atoms/files/conclusions_dpa_investigation_nike_running_app.pdf*

EU Agency for Fundamental Rights issues report on surveillance by intelligence services

A recently published FRA (European Union Agency for Fundamental Rights) research paper suggests that there is a need to adapt and strengthen the relevant legal surveillance frameworks in the EU Member States. Although some reforms have already been made, more work needs to be done to improve accountability and oversight.

The research maps the 28 EU Member States' legal frameworks related to surveillance and provides an overview of existing fundamental rights standards. It focused on oversight mechanisms and on remedies available to individuals alleging infringements of their right to privacy. The research does not examine surveillance techniques as such. It reviews how current legal frameworks enable the use of such techniques, and explores the crucial role specialised bodies play in overseeing the work of intelligence services.

The FRA collected data and information through desk research in all 28 EU Member States. Additional information was gathered through exchanges with key partners, including a number of FRA's national liaison officers in the EU Member States, specialised bodies, and individual experts.

The report says that almost all EU Member States have established at least two different intelligence services bodies, one for civil and one for military matters oversight. FRA findings show that, compared with other data processing activities and data controllers of the public and private sector, DPAs in seven Member States have the same powers over intelligence services as over all other data controllers. In 12 Member States, DPAs have no competence over intelligence services, and in nine their powers are limited.

In Member States in which DPAs and other expert oversight bodies share competence, a lack of cooperation between these may leave gaps resulting from fragmented responsibilities. In Member States where DPAs lack competence over intelligence services, the oversight body is responsible for ensuring that privacy and data protection safeguards are properly applied.

- *See http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services*

Russia's new law overrules judgments by European Court of Justice

Russia's lower house of parliament, the Duma, voted on the law at the beginning of December. The measure was fast-tracked, giving the constitutional court the right to declare international court orders unenforceable in Russia if they contradict the constitution, the BBC reports. Russia ratified the European Convention on Human Rights in 1998. The law is specifically aimed at "protecting the interests of Russia" in the face of decisions by international bodies responsible for ruling on human rights.

A human rights activist recently sued Google Russia for allegedly reading his email. Google's user agreement states that the company conducts an automatic content analysis 'to provide you with personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection'. The claimant intends to pursue the case at the European Court of Human Rights.

- *See http://www.ejiltalk.org/blockbuster-strasbourg-judgment-on-surveillance-in-russia/ and http://www.bbc.co.uk/news/world-europe-35007059*

Portugal: New rules on intragroup transfer agreements

The Portuguese Data Protection Authority (CNPD) has issued a deliberation in which, in certain circumstances, it considers intragroup agreements to be a valid mechanism for data transfers outside the European Union. This deliberation follows the ECJ's recent decision which invalidated the EU-US Safe Harbor.

The CNPD considers intragroup agreements to be a valid mechanism for legitimising international data transfers to third countries which do not provide for an adequate level of protection of the data, provided they comply with the European Commission Standard Contractual Clauses, as described by CNPD. With this deliberation, CNPD seeks to speed up the process towards obtaining the authorisation for personal data transfers outside EU territory.

- *CNPD's deliberation (in Portuguese) is available at: https://www.cnpd.pt/bin/decisoes/Delib/20_1770_2015.pdf*

Reported by Vieira de Almeida & Associados, email: vieiradealmeida@vda.pt

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