GPEN: A growing network but how much 'enforcement'?

Colin J. Bennett

October 2015

GPEN: A growing network but how much 'enforcement'?

Colin J. Bennett assesses what we can expect from DPAs' international cooperation and what has been achieved so far.

Amid all the controversy concerning the European General Data Protection Regulation (GDPR) and the controversies over the "One-Stop Shop," there has been relatively little attention paid to the gradual emergence of the Global Privacy Enforcement Network (GPEN).[1] It is difficult to find any scholarly work about GPEN, nor much journalistic commentary.[2] This could be a case of a "below the radar" effort at cross-national cooperation that is beginning to be effective precisely because there has not been much publicity.

GPEN is a network of privacy enforcement authorities. According to the 2014 Annual Report, the network comprises 53 privacy enforcement authorities in 39 jurisdictions around the world. It includes the specialised data protection authorities (DPAs) on the European model, and crucially also the US Federal Trade Commission (FTC).[3] It was established in 2010, as a result of a recommendation by the OECD, and successive resolutions at the International Conference of Data Protection Commissioners from the International Enforcement Co-ordination Working Group.[4]

These efforts culminated in a Framework for Enforcement Cooperation that was adopted at the International Conference in Mauritius in 2014.[5] This agreement is a kind of memorandum of understanding designed to encourage greater cooperation and coordination. It is non-binding, and DPAs can decide whether or not to participate. The agreement is based on principles of reciprocity, confidentiality and cooperation.[6]

The practical mechanism to realise these goals will be GPEN, whose mandate is to promote cooperation among privacy enforcement agencies by: exchanging information and expertise; encouraging training; promoting dialogue; maintaining processes useful to bilateral or multilateral cooperation; and supporting specific enforcement activities. It is split into an Atlantic and a Pacific group, which both schedule an increasing number of teleconferences on different matters. The GPEN is run by a small steering committee now comprising representatives from Canada, Israel, the UK and the United States.

The GPEN annual report indicates the following goals for 2015: further growth in membership; a third annual enforcement sweep; new capacity building opportunities such as secondments, training and employment exchanges; the enhancement of links with similar groups, such as APEC; and the finalisation of a secure online enforcement coordination platform and information sharing system. This latter would allow GPEN members to alert other members about current investigations and to discover whether others are investigating the same company or practice.[7]

In many ways the GPEN is a logical extension of 40 years of international collaboration on privacy protection issues. The community of DPAs has reached a critical mass where more professional methods for sharing expertise and information make perfect sense. In the past, there has been an unnecessary duplication of effort on many issues, resulting in a patchwork approach to investigations and diverse findings on similar cases. DPAs have limited resources, and there is no reason why they should expend time and effort on research and investigative efforts if their colleagues in other jurisdictions have already done the work. How many reports do we actually need about the privacy implications of drones, automatic license plate recognition, the connected car, genetic data banks and so on?

But most of this activity relates to cross-national learning: the sharing of information and expertise to minimise transaction costs. This aspect of the network's collaboration is generally uncontroversial and invaluable for newer authorities to draw lessons about best practice from those with greater experience.

But what about actual enforcement? Is GPEN a network through which privacy enforcement authorities can learn of the experiences of authorities in other jurisdictions? Or is it an "enforcement network"? So far, the evidence suggests that it is the former? Can it become the latter?

There have been a few encouraging examples in recent years where DPAs have collaborated on enforcement initiatives. But closer inspection reveals that these actions are not all the same type of "enforcement" and have different motivations, sources and methods.

The first example is the enforcement that might arise from the "global sweep" exercises.[8] These are broad cross-national research exercises designed mainly to recreate the consumer experience and to assess the transparency of personal information practices against a common set of indicators. So far, there have been three privacy sweeps. The first was in 2013 about website privacy policies, the second was on mobile apps and the most recent sweep (May 2015) focused on childrens' apps [see p.23].[9] The numbers of DPAs involved has increased quite dramatically, and there has generally been good press coverage. Some DPAs have taken enforcement action, depending on their own priorities and powers. But the global sweep is explicitly not described as an "investigation" nor "intended to conclusively identify compliance issues or possible violations of privacy legislation." It has been described as a "non-investigative" investigation.

These exercises are clearly valuable, and provide useful high-level overviews of the main compliance issues. They also accustom different authorities to the value of working together and help build valuable personal connections, especially among the staff responsible for compliance and investigations. But they are limited to the extent that they cannot test the full range of compliance issues. The measurement of transparency from the standpoint of the consumer is perhaps the most straightforward compliance metric.[10]

A second form of enforcement collaboration might arise from joint complaints. An outside group, for example, might lodge the same complaint against the same global company simultaneously to multiple authorities. Rather than investigate individually, the authorities might then pool resources and conduct joint investigations. One illustration is the joint complaint lodged by Privacy International against the financial messaging service, Swift, in 2006.[11] The DPAs then referred the case to the Article 29 Working Party, which issued an advisory opinion on the legality of SWIFT's operations. There were then follow-up investigations by the Belgian and Dutch DPAs.[12] The SWIFT case is, however, a fairly isolated example where a privacy advocacy group was able to launch the same complaint to several DPAs at the same time about the same set of issues. The privacy advocacy network, at least outside the United States, does not generally have the resources to coordinate complaints on an international scale.[13]

A third form of enforcement action stems from joint expressions of concern. In these cases, the suspicion of non-compliance may stem from a number of sources: media stories, activism by privacy advocacy groups, or even from a company's own promotions. In 2010, the DPAs of Canada, France, New Zealand, UK, Germany, Israel, Italy, Spain and the Netherlands sent a joint letter to Google expressing strong concerns about its roll out of new technological applications without sufficient consultation.[14] In 2013 and in a similar vein, a broader coalition of 36 DPAs sent a letter to Google asking a series of questions about Google Glass.[15]

A broader coalition worked under the auspices of GPEN earlier in 2015 to pressure the operators of a Russian website (www.inssecam.org) that was streaming live video footage from home and commercial surveillance cameras. The coalition came together quickly and called on the company to take down the website with threats of further enforcement action.[16] This example illustrates the potential for swift action against the most egregious violations of privacy rights. These "just explain" letters, whether written in confidence or publicly, can be very effective instruments, and can help prepare the ground for more proactive enforcement.

A fourth, and rarer, form of enforcement is where DPAs actually conduct joint investigations. A fine example is the joint investigation of WhatsApp by the Canadian and Dutch DPAs in 2013. Both authorities worked closely together, but issued separate reports and pursued follow-up enforcement actions separately, because the Dutch DPA, unlike the Canadian Privacy Commissioner, has the power to impose sanctions.[17] Also in 2013, six European DPAs launched coordinated, but separate, investigations into Google's new privacy policy, which permitted sharing of personal data across platforms. This culminated in fines levied in France, Spain and the Netherlands, although issues are far from resolved.[18]

A final model is where jurisdictional limitations prevent the full enforcement of domestic data protection law against companies that reside in different locations. There was an interesting example of collaboration between the Canadian Privacy Commissioner and the FTC in a case involving a US-based company called Accusearch, a data brokerage firm. The OPC's initial investigation was taken up by the FTC, and later by the US District Court which ultimately found against the company.[19] Another example is the ongoing enforcement action against the Romanian-based website, www.globe24h.com, which was republishing often sensitive legal decisions and demanding a fee for removal. The OPC has cooperated with the Romanian Data Protection Authority to secure the removal of the offending material and pursue further enforcement.[20]

It should also be noted that there is a considerable variation in legal requirements for data breach notification, enforcement and sanctions. Data breaches can have global consequences. Can DPAs with weaker enforcement powers leverage greater compliance by "shopping around" for those jurisdictions with wider powers of enforcement and sanction?

> Can DPAs with weaker enforcement powers leverage greater compliance by "shopping around"?

In summary, "enforcement" collaboration can appear in a number of different guises: bilateral or multilateral; with or without complaints; proactive or reactive; against one company or an entire industry; and with or without the imposition of sanctions.

So what are the barriers to further enforcement cooperation? I think they are legal, economic, organisational and cultural.

DPAs operate, of course, within very different constitutional and administrative traditions. They do not all have the same set of legal tools. Some have enforcement and sanction powers; others operate more as ombudsmen. It is important not to overstate these differences, however. To be sure, different legal frameworks dictate somewhat different investigatory and enforcement styles and procedures. And of course there are often tricky issues with being able to share the confidential information discovered during the course of investigations. Significant progress seems to have been made within

GPEN through the establishment of the new secure platform for the sharing of information on current investigations and enforcement activities.

Secondly, there are obviously resource constraints. DPAs have varying sets of resources, and have to make tough decisions about how to allocate moneys and staff, often in tight budgetary circumstances. I have observed over the years that it is often the broader policy mandate that tends to get cut first, in favour of the more pressing need to investigate complaints and clear 'backlogs.'

DPAs also have to be seen by local constituencies as taking care of domestic matters. Their legitimacy is rooted in domestic legislation and in the need to be seen to be responding to the inquiries and complaints of local citizens and to be giving practical advice to local public and private organisations. Joint enforcement on the world stage, perhaps against well-financed global corporate actors, can not only put a strain on budgets, but also risk criticism that domestic matters are being ignored.

There are also some clear organisational constraints. Some DPAs are reasonably large; others quite small. Some have responsibility for other issues, such as freedom of information (as in Canada) or the Do-Not-Call register (as in Singapore). Some are truly "independent"; others less so. And some, of course, operate within federal structures and need to be sensitive to the powers and responsibilities of their colleagues in other sub-national jurisdictions as well as at the national levels. Such questions can be particularly tricky in Canada and Australia.

Finally, and perhaps most importantly, there are also some cultural barriers. Collaboration on enforcement requires a change in philosophy and outlook among many DPAs. It requires a change in outlook from the "I" to the "we", and a willingness to subsume the demands of local political contingencies in favour of a joint approach with perhaps different outcomes than would be reached if actions were taken separately. The transition from the domestic to the international governance of privacy is therefore as much about fostering that trust and community within the privacy enforcement authorities, as it is about interpreting the law.

Collaboration on enforcement also requires some DPAs, often used to being in the limelight in their own jurisdictions, to sometimes take a back seat. And that is often difficult, as there is a natural tendency to want to claim credit for successful enforcement actions. Collaboration often also requires a more flexible attitude to the law. We perhaps need more data protection and privacy commissioners who take less of a "strict constructionist" approach to data protection law, and who are willing to push the boundaries of their statutory responsibilities and jurisdictions. I have also argued that collaboration requires (in some countries) a better relationship with the network of civil society actors that advocate for privacy, and a recognition that a creative tension between more radical activist groups and the official DPAs can do a lot to advance the cause.[21]

The illustrations of enforcement collaboration cited above are not meant to be exhaustive, but I would conclude a few things from this brief review.

There has been an increase in the frequency, type, and quality of international enforcement actions by DPAs. The illustrations above suggest that there is now precedent for all kinds of collaboration on joint enforcement actions, and nobody has argued that cooperative enforcement by DPAs is somehow outside their powers or competence. It is now commonly recognised that when more than one DPA speaks on an issue, they tend to get more attention, than if they act alone. Collaboration between DPAs is therefore becoming institutionalised within the "governance of privacy".[22]

It is also worth noting that GPEN is one of a number of overlapping networks of DPAs organised either on regional, linguistic or functional lines. These include: the Asia-Pacific Privacy Authorities (APPA); the Association Francophone des Autorités de Protection des Données Personelles; the International Working Group on Data Protection in Telecommunications; and the APEC cross-border privacy enforcement arrangement.

These intersecting networks of DPAs are layered over, or within, or under, or beside (pick the preposition) the more established international regimes that have been part of the privacy and data protection scene for a long time: the European Union, the OECD, the Council of Europe, international standards organisations, the United Nations and others.

The divisions of labor and responsibility within the international system of privacy governance are getting extraordinarily, and perhaps unnecessarily, complicated.

With that in mind, it is also important to remember that most of the enforcement actions noted above were not inspired or initiated by formal collective decision-making. Rather they arose because one or two lead authorities decided to act, did the necessary legal and technical research, and then sought support from colleagues overseas. I do not want to belittle the importance of more formal structures and processes of information-sharing and collaboration between DPAs. But we should also not forget that much has already been achieved through appropriate action at the right time, with a strong "can-do attitude" by one or two lead authorities. It would be a shame if the network became so mired in procedure that it could not act spontaneously when obvious violations of privacy arise.

AUTHOR

Professor Colin J. Bennett, Department of Political Science, University of Victoria, BC, Canada.
Email: cjb@uvic.ca, www.colinbennett.ca

INFORMATION

This article is based on a presentation to the Global Privacy Enforcement Network's Asia-Pacific Section on 4 August 2015. My thanks to Blair Stewart for his comments on an earlier draft.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Safe Harbor invalid: What to expect after the ruling?

Sarah Cadiot and **Laura De Boel** explain what businesses can do to enable transfers to the US.

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued a landmark judgment[1] invalidating the European Commission's Decision of 2000[2] which recognised the adequacy of the EU-U.S Safe Harbor framework (Safe Harbor). In addition to the invalidation of this adequacy decision, the CJEU upheld the power of national Data Protection Authorities (DPAs) to independently investigate international data

Continued on p.3

ECJ clarifies meaning of territorial scope in DP Directive

Hungarian data protection law applies to a company's activities in Hungary, although registered in Slovakia. **Andrea Klára Soós** reports.

On 1 October 2015, the European Court of Justice (ECJ) published its decision in case No. C-230/2014[1]. In this decision the ECJ followed the argumentation of Advocate General Pedro Cruz Villalón[2] and came to the conclusion that the principle of establishment should be applied by the authorities of other EU Member States. Consequently, a data controller could be investigated

Continued on p.5

Issue 137 **October 2015**

INTERNATIONAL report

ISSUE NO 137 **OCTOBER 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
Sarah Cadiot and **Laura De Boel**
Wilson Sonsini Goodrich & Rosati, LLP, Belgium
Andrea Klára Soós
Soós law firm, Hungary
Hiroshi Miyashita
Chuo University, Japan
Yuli Takatsuki and **Phil Lee**
Fieldfisher Silicon Valley, US
Whon-il Park
Kyung Hee University Law School, South Korea
Patricia Muñoz-Campos
Bird & Bird, Spain
Andra Giurgiu
University of Luxembourg, Luxembourg
Gertjan Boulet and **Paul De Hert**
Vrije Universiteit Brussels, Belgium
Colin J. Bennett
University of Victoria, BC, Canada
Sinta Dewi Rosadi
Padjadjaran University, Indonesia

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

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

comment

Safe Harbor collapses – but data transfers will continue

The Court of Justice of the European Union's recent landmark decisions on Weltimmo and Safe Harbor (p.1) strengthen individual Data Protection Authorities' powers. The EU DPAs can now make decisions whether to suspend transfers to the US – but the EU Commission immediately said that a coordinated approach is needed to avoid fragmentation. The Chair of the Article 29 DP Working Party, Isabelle Falque-Pierrotin, President of France's CNIL agreed – but will all DPAs share this view? DPAs now have to come up with a plan of action for now until a new regime for EU-US transfers can be agreed.

The EU Commission says that it will step up negotiations with the US on 'Safer Harbor' and is still confident that the EU Data Protection Regulation can be agreed this year. One aspect of the reform is the ambitious plan for a One-Stop-Shop (p.16). It will require enhanced cooperation between the regulators – something that is already taking place on Binding Corporate Rules and, to some extent, within the DPAs' enforcement network (p.19).

The court's decision in the Weltimmo case (p.1) states that DP law of a Member State may be applied to a foreign registered company if it has activities in a country, for example, operating in the native language of the country and has representatives in that country, even if not headquartered there. This decision is likely to have a huge impact on companies operating on the Internet. The Safe Harbor / Max Schrems case is essentially about US surveillance with major impact on transfers (p.1). Key US legal provisions are discussed from p. 11 onwards.

The nearly adopted Umbrella Agreement signifies an important step in rebuilding trust in EU-US data flows. However, the European Parliament's approval is still needed and it has not been satisfied with the secretive negotiation process (p.7). The same secrecy surrounds the EU DP Regulation Trilogue process – there is no information in the public domain.

Asia is on the world privacy map now due to its Big Data related actions. Read about Japan's new law (p.8) which is intended to win it EU adequacy status, while South Korea's initiatives are in the context of its "Creative Economy" business synergy programme (p.15). In addition, there is a new Indonesian draft regulation, which affects both private and public sectors (p.27). By contrast, India's Supreme Court may play a role in making progress on a timetable for an ID card-related privacy law but the slow and confusing turning of legal wheels means that an Indian privacy law looks likely to be delayed until an unknown future (p.24).

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.

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