THE GLOBAL ENFORCEMENT PRIVACY NETWORK:

A GROWING NETWORK BUT HOW MUCH 'ENFORCEMENT'?[1]

Colin J. Bennett

Department of Political Science, University of Victoria, BC, Canada

www.colinbennett.ca

cjb@uvic.ca

Amid all the flurry of activity 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).[2] It is difficult to find any scholarly work about GPEN, nor much journalistic commentary.[3] So 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 word. It includes the specialized data protection authorities (DPAs) on the European model, and crucially also the US Federal Trade Commission (FTC).[4] 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 which produced a parallel iniative for a Global Cross Border Enforcement Arrangement.[5]

The GPEN is run by a small steering committee now comprising representatives from Canada, Israel, the UK and the United States. Its 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. Through the GPEN website, users have access to the International Privacy Law Library operated by

---

[1] A presentation to the Global Privacy Enforcement Network's Asia-Pacific Section on August 4, 2015. My thanks to Blair Stewart for his comments on an earlier draft.

[2] https://www.privacyenforcement.net

[3] One notable exception is an earlier article by Charles D. Raab, "Networks for Regulation: Privacy Protection in a Changing World," Journal of Comparative Policy Analysis Vol. 13, No. 2: 195-213 (April 2011)

[4] https://www.fcc.gov/document/fcc-joins-global-privacy-enforcement-network

[5] International Conference of Privacy and Data Protection Commissioners, Working Group Reports at: http://icdppc.org/document-archive/working-group-reports

the Australasian Legal Information Institute (Austlii). It is split into an Atlantic and a Pacific group, which both schedule an increasing number of teleconferences on different matters. To date, its most significant enforcement action has been the "mobile apps" sweeps conducted over the last three years (see below).

The GPEN annual report indicates the following goals for 2015: further growth in membership; the third annual enforcement sweep; new capacity building opportunities such a secondments, training and employment exchanges; the enhancement of links with similar groups, such as APEC; and the finalization 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.[6]

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 makes perfect sense. In the past, there has been an unnecessary duplication of effort on many issues. 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 minimize 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, noted above, is the enforcement that might arise from the "global sweep" exercises.[7] This is essentially a broad cross-national research exercise 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 web site privacy policies, the second was on

[6] GPEN Annual Report 2014 at: https://www.privacyenforcement.net/node/513

[7] "Global privacy sweep raises concerns about mobile apps," Privacy Commissioner of Canada News Release at: https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp

mobile apps and most recent sweep (May 2015) focused on childrens' apps.[8] 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.[9]

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.[10] 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.[11] 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 practices. The privacy advocacy network, at least outside the United States, does not genrally have the resources to coordinate complaints on an international scale.[12]

A third form of enforcement action stems from joint expressions of concern. On 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

---

[8] https://www.priv.gc.ca/media/nr-c/2015/nr-c_150511_e.asp

[9] See also out analysis of the transparency of policies of social networking sites at: www.catsmi.ca

[10] "Privacy International Extends Legal Action against Banking Giant SWIFT," July 10, 2006 at: https://www.privacyinternational.org/?q=node/534

[11] EU Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT) at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf

[12] See my anlaysis of this network in *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008).

out of new technological applications without sufficient consultation.[13] 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.[14]

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.[15] 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 publically, 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.[16] 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.[17]

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.[18] The OPC filed an amicus brief in the case. The potential for investigation in one country and enforcement in another is also apparent with respect to data breaches. There is a considerable variation

---

[13] Letter to Google Inc. CEO at: https://www.priv.gc.ca/media/nr-c/2010/let_100420_e.asp

[14] "Data Protection Authorities urge Google to address Google Glass concerns," at: https://www.priv.gc.ca/media/nr-c/2013/nr-c_130618_e.asp

[15] "Letter to operators of webcam website" November 21, 2014 https://www.priv.gc.ca/media/nr-c/2014/let_141121_e.asp

[16] "WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities," OPC News Release January 28, 2013 at: https://www.priv.gc.ca/media/nr-c/2013/nr-c_130128_e.asp

[17] "Six European privacy regulators launch investigations of Google's privacy policy," *Computerworld* April 2, 2013 at: http://www.computerworld.com/article/2496107/data-privacy/six-european-privacy-regulators-launch-investigations-of-google-s-privacy-policy.html

[18] *Accusearch Inc v. Federal Trade Commission* at: https://www.priv.gc.ca/leg_c/court_p_05_e.asp

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?

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, organizational 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, a problem that seems to have been resolved 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 in often tight budgetary circumstances. I have observed over the years that it is often the broader policy mandate that tends to get cut first, in favor of the more pressing need to investigate complaints and clear 'backlogs.'

DPAs also have to be seen by local constituencies of taking care of domestic matters. Their legitimacy is rooted in domestic legislation and in the need to be seen to be responding to the inquries and complaints of local citizens and to be giving practical advice to local public and private organizations. 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 *organizational* 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, I think 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 favor 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.[19]

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. In the history of the "governance of privacy" we are perhaps entering a new era, where collaboration by DPAs on enforcement activities will become the norm.[20] It is now commonly recognized 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 institutionalized.

It is also worth noting that GPEN is one of a number of overlapping networks organized either on regional, linguistic or functional lines. The intersecting networks of DPAs is layered over, or within, or under, or beside (pick the preposition) the more established international regimes that have been part of the international data protection landscape for a long time: the European Union, the Organisation for Economic Cooperation and Development, the Council of Europe, a number of international standards organizations, 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 initiatied 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. The joint letters sent to Google are an excellent case in point. I do not want to belittle the importance of

---

[19] See Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance*, (Cambridge: MIT Press, 2008)

[20] See Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006)

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 strong leadership 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.