UN PRIVACY RAPPORTEUR SETS HIGH GOALS

GRAHAM GREENLEAF

(2016) 140 *Privacy Laws & Business International*

Report 10-12, 30 April 2016

[2016] *UNSWLRS* 55

UNSW Law
UNSW Sydney NSW 2052 Australia

UN privacy Rapporteur sets high goals

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

Published in (2016) 140 *Privacy Laws & Business International Report*, 10-12, April 2016

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

'The beginning of the judicial end for mass surveillance'

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

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

Following this approach, he argues that the UK Government's proposals for the *Investigatory Powers Bill* 'prima facie fail the benchmarks set by the ECJ in *Schrems* and the ECtHR in *Zakharov*'. Rather than see the UK's legislation before either of these courts, the SRP

---

[1] United Nations *Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*. Human Rights Council, Thirty-first session, 8 March 2016

[2] For background to the appointment, see Graham Greenleaf 'The UN Special *Rapporteur*: Advancing a Global Privacy Treaty?' (2015) 136 *Privacy Laws & Business International Report*, 7-9

[3] *Roman Zakharov v Russia* [2015] ECHR 1065 (4 December 2015) <http://www.bailii.org/eu/cases/ECHR/2015/1065.html>

encourages the UK government to 'set a good example and step back from taking disproportionate measures' particularly because of 'the huge influence that UK legislation still has in over 25% of the UN's members states that still form part of the Commonwealth, as well as its proud tradition as a democracy which was one of the founders of leading regional human rights bodies such as the Council of Europe.'

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

'First small steps towards cyberpeace?'

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

One element of 'cyberpeace' of which he clearly approves is the 'wise restraint' shown by the Netherlands government in its January 2016 announcement that it formally opposes the introduction of backdoors in encryption products.[4] Concerning the ongoing *Apple v FBI* case concerning whether Apple could be forced to develop software to defeat security features on its phones, the SRP agreed with the separate statement by the UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein, arguing that 'A successful case against Apple in the US will set a precedent that may make it impossible for Apple or any other major international IT company to safeguard their clients' privacy anywhere in the world.'[5]

Genetics, biometrics and privacy

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

Anonymisation, Open Data and Big Data analytics

Despite his concerns about State mass surveillance, the SRP regards corporate use of personal data as a comparable threat: 'In the early days of digital computers, one of the main concerns was the use of personal data by the state and the state's abilities to correlate data held in various sources to form a detailed picture of an individual's activities and assets. In 2016 it

---

[4] Tweede Kamer, 'Kabinetsstandpunt encryptie' 4 January 2016 <http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015>

[5] UNHCHR Media release 'Apple-FBI case could have serious global ramifications for human rights: Zeid' 4 March 2016 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E>

would seem that much more data is held on the individual by corporations than that held by the state.' Not only has the data available for profiling increased by an order of magnitude in 25 years but there is also 'not enough evidence available to properly assess the risk inherent in purportedly anonymised data which can be reverse engineered in a way such to be linked to an identified or identifiable individual.' The reversibility of supposed de-identification/anonymisation is a major theme of the Report. He takes a very skeptical view of the 'Open Data' movement and its demands for open access to public data sets, because they then become susceptible to Big Data analytics. 'It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide.'

Back to basics: The purpose-specification principle

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

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

Carrots and sticks

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

The role of international privacy agreements

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

---

[6] Department of Health, Education and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U S Govt. Printing Office, Washington USA 1973 at p. 41

[7] 37th International Conference of Data Protection and Privacy Commissioners *Resolution on Cooperation with the UN Special Rapporteur on the Right to Privacy,* Amsterdam, 27 October 2015

The US FTC abstained in 2013 and 2015 to the resolution 'which relates to matters outside its jurisdiction'.

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

The SRP identifies the updating of existing international legal instruments as 'an essential starting point'. Although he notes that there 'appears to be a consensus among several stakeholders' that a new protocol to ICCPR article 17 is desirable, he considers that the timing of this might depend on the adoption or a new international agreement on other privacy-related issues such as jurisdiction and territoriality in cyberspace. However, he does not envisage 'one new global all-encompassing international convention covering all of privacy or Internet governance' but rather 'incremental growth of international law and thus the clarification and eventually the extension of existing legal instruments as well as even, in the mid to long term, the development of entirely new legal instruments.'

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

Future directions: What ongoing UN role in data privacy?

Subject to his resource and time constraints, the SRP has embarked on a 'Ten Point Action plan' of increasing awareness and engagement, detailed in the Report.[9] Few outsiders to the UN system probably realise that the prestigious positions of Special Rapporteurs come without any resources to carry out their daunting tasks: no staff, not even a travel budget (except perhaps when summonsed to the Human Rights Council). The Report explains this in detail, and that it is vital to obtain 'extra mural funding outside UN sources'. So far, academic sources have produced one full-time post-doctoral researcher, much assistance from academia and NGOs (including some part-time volunteers), and negotiations with DPAs which may generate some seconded staff. Negotiations with governments and the private sector are intended to follow. This 'first SRP' is actively pursuing the building up of such capacity 'to ensure sustainability of work on privacy protection'. This has the potential to benefit this SRP, but also his successors if this mandate is renewed. However, it has be to be borne in mind at all times, when considering what a SRP achieves, what resources they did or did not obtain, and the source of those resources.

[8] Graham Greenleaf 'International DP agreements after the GDPR and Schrems' (2016) 139 PLBIR 12-15

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