Towards multilateral standards for surveillance reform

Ian Brown, Prof. of Information Security and Privacy
Oxford Internet Institute, University of Oxford
@IanBrownOII

Motivation

- Snowden revelations have led to some public unease, but limited political pressure for reform of foreign intelligence surveillance (cf USA Freedom Act) – now contrasted with renewed public concerns over terrorism
- But, status quo threatens public trust in Internet, its status as a free and global system, US-EU cooperation – including on law enforcement and counter-terrorism – and problems with international human rights law
  - "Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law."

Data localisation

- German interior minister: “whoever fears their communication is being intercepted in any way should use services that don't go through American servers.”
- Snowden: “you should never route through or peer with the UK”
- Brazil & Russia – considered or passed laws requiring citizens’ data held within country. *Digital Rights Ireland* and Art 29 WP on retained communications data
- Regional data centres – limited impact given expansive American jurisdiction (Microsoft case – see Irish govt amicus brief)
- Norwegian domains .sj and .bv – Iceland, Swiss discussion of “data havens”

UN High Commissioner for HR

- “Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights” §20
- “overarching principles of legality, necessity and proportionality” §23
  - “secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of “law” §29
- “sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17” §27
- “Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness” §30

United Nations

- General Assembly: “Calls upon all States…To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law” (A/RES/68/167)
- HR Cmtte: Concluding Observations on USA (2014). Inter-State complaint? (Scheinin)
- IGF 2014: “Civil society managed to get many of these issues on the conference’s agenda but governments chose to ignore them.” -Sherif Elsayed-Ali, Deputy Director of Global Issues at Amnesty International

Four main reform proposals

- 46 recommendations of President's Review Group on Intelligence and Communications Technologies (some limits on collection and analysis of data relating to non-US persons) – some implemented by PPD-28
- European Parliament report (but member states have exclusive competence on national security)
- 13 necessary and proportionate principles (civil society) – need for more discussion on operational impact
- 5 principles for surveillance reform (well-known Internet companies) – says little about privacy from private sector

Next steps

- The democracies – we suggest beginning with the North Atlantic allies – could ensure legitimacy and public trust by developing an agreement on effective, necessary and proportionate surveillance measures, with business and civil society
- Germany would be a natural leader within EU, and economic pressures may encourage US to engage
- Also likely to be continued reform of national surveillance laws (esp. post-Paris attacks), including with reauthorisation of US PATRIOT Act provisions this year on roving wiretaps, business records, and lone actor surveillance