International Working Group
on Data Protection
in Telecommunications

675.54.10

**Working Paper**

# Towards International Principles or Instruments to Govern Intelligence Gathering

61st Meeting, 24-25 April 2017, Washington D.C. (USA)

## Scope

There have been increasing calls for an international instrument setting out agreed principles for the conduct of intelligence activities. This paper summarises some of those calls and presents the case for data protection authorities to participate in this dialogue. The paper proposes an initial set of principles that it is hoped could form the basis for such an instrument.

## Stocktake on recent developments

Historically, intelligence activities have been conducted in secret, and Governments have seldom acknowledged the nature or extent of those activities. They have been subject to no internationally agreed standards, and have often been undertaken under opaque legal authority.

In recent years, partly in response to the revelations of Edward Snowden in 2013, there has been increased public awareness and discussion of the tensions in the digital arena between States' interest in national security and individuals' rights to privacy, as well as unease and global debate on where the proper balance is to be struck. Themes have emerged from public debate including the desire for limits on the use of technology by intelligence agencies to gather personal information, the regulation and oversight of intelligence agencies' use of telecommunications technologies and access to networks and the options for building global consensus on promoting and protecting the right to privacy in the light of these developments.

United Nations Member States have expressed concern at revelations of intelligence agency practices involving the collection, storage, retention and use of telecommunications information, including digital communications facilitated by the Internet.[1] Unease about these revelations was compounded by a lack of clarity in the application of existing international human rights standards, including the right to privacy, to the activities of intelligence agencies in the digital sphere. These issues led to the United Nations General Assembly Resolution, *The right to*

[1] See, for example, United Nations General Assembly and Human Rights Council debate on the right to privacy in the digital age (2013).

*privacy in the digital age*[2] and the creation of a new mechanism, the Special Rapporteur on the Right to Privacy (SRP), in late 2014.

Since the establishment of the SRP, two substantive resolutions have been adopted by the UN: by the General Assembly in December 2016 (A/RES/71/199[3]) and by the Human Rights Council in March 2017 (A/HRC/34/7[4]). These resolutions build upon previously agreed language and develop the scope of obligations of States in relation to actions of corporations. The Council's resolution also, for the first time, recognises that any grounds for interference with the right to privacy should comply with the principles of legality, necessity and proportionality.

It is timely for data protection authorities to once again explore these issues and promote approaches to improve the governance of intelligence gathering in accordance with principles that reconcile respect for the right to privacy with the legitimate needs of national security.

*Calls for consensus on international standards and the right to privacy in the digital age*

Steps have been taken to encourage consensus on the application of international law to the right to privacy in the digital age, including appropriate mechanisms for the oversight of activities of intelligence agencies.

For example, in 2013, the United Nations established a new Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (GGE). The GGE reported to the General Assembly in July 2015 on suggested norms of behaviour and other issues relevant to international security in cyberspace, including that:[5]

- *In their use of Information and Communications Technologies (ICTs), States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.*
- *Existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.*
- *States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.*
- *The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour.*

---

[2] United Nations General Assembly, 18 December 2013, A/RES/ 68/167. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

[3] United Nations General Assembly, Resolution 71/199 – "The right to privacy in the digital age". Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199

[4] United Nations General Assembly, Human Rights Council, Resolution A/HRC/34/7 – "The right to privacy in the digital age". Available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement

[5] United Nations, Report of the Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, A/70/714. Available at: http://undocs.org/A/70/174

The GGE report was subsequently welcomed by the China-United States of America Cyber-Security Agreement (2015), which agreed to establish a senior experts group for further discussion on this topic.[6] The GGE is due to report again to the General Assembly in 2017. The GGE will report on:

- work to build common understanding of existing and potential threats in the sphere of information security;
- possible cooperative measures to address them; and
- how international law applies to the use of ICTs by States including rules, norms and principles of responsible behaviour of States.

In 2013 the International Working Group on Data Protection in Telecommunications issued a working paper on the Human Right to Telecommunications Secrecy which urged governments:

1. To recognise telecommunications secrecy as an essential part of the globally acknowledged human right to privacy;
2. To strengthen telecommunications secrecy as a human right in an international convention. Restrictions should be limited to what is strictly necessary in a democratic society;
3. To agree on international rules limiting government access to data stored by Internet service providers and signals intelligence on the Internet;
4. To provide for greater transparency and public accountability of government agencies as to the results of lawful interceptions; this includes transparent rules on classification and declassification;
5. To ensure that every data subject regardless of nationality has the right to be notified ex post, to have his data deleted and corrected and of access to justice;
6. To allow and encourage citizens to freely research, create, distribute and use tools for secure communications; no citizen should be monitored simply on the ground that he or she is using such tools;
7. To ensure effective and independent oversight with regard to surveillance activities carried out by police and intelligence agencies or on their behalf by private processors.[7]

Also in 2013, the International Conference of Data Protection and Privacy Commissioners resolved to call upon governments to advocate the adoption of an additional protocol to Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[8]

*The use of technology by intelligence agencies*

The inaugural International Intelligence Oversight Forum (IIOF) was hosted by the SRP in 2016 and concluded that several themes have emerged concerning the use of technology by

---

[6] The White House, Fact Sheet, President Xi JinPing State Visit, 25 September 2015. Available at https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

[7] Working paper on the Human Right to Telecommunications Secrecy, 2013: https://datenschutz-berlin.de/attachments/993/WP_Human_Right.pdf?1382357419

[8] Resolution on anchoring data protection and the protection of privacy in international law, Warsaw, 2013, https://icdppc.org/wp-content/uploads/2015/02/International-law-resolution.pdf

governmental agencies. These themes include: the need for standardisation of terms and language; the need for confidential and open dialogue to better understand national systems, their similarities and differences (as well as collection of good and bad practices); the need for a more evolved, less secretive discussion of the work of intelligence agencies and how to structure oversight of them; and the need for safeguards and remedies – preferably on an international level (including accountability and transparency). The next IIOF, in late 2017, will seek to build on this work.

*Research*

Research initiatives have also emerged in response to these developments. For example, the European Union Agency for Fundamental Rights (FRA) commenced, at the request of the European Parliament, research to assess how laws relating to national intelligence agencies are being implemented in seven Member States: Belgium, Germany, Italy, France, the Netherlands, Sweden and the United Kingdom.[9] The mapping of legal frameworks was published in 2015 and will be followed, in October 2017, with a report combining analysis of these laws with how they translate into practice and opinions on ways to better safeguard fundamental rights, including the right to privacy.[10]

In 2016, the SRP commenced research, building on research initiatives at the University of Groningen, into a new MAPPING Project[11], which will explore whether it is possible to devise a legal instrument specifically on surveillance activities by government agencies (including both law enforcement and intelligence agencies). This work will also be continued in 2018.

*National initiatives*

At the national level, new laws are emerging to govern the activities of intelligence agencies, including principles for oversight of these activities. For example, in the United States of America, the Central Intelligence Agency has developed principles to guide signals intelligence activities[12] along with Presidential Policy Directive 28: Signals Intelligence Activities.[13] In New Zealand, new legislation has been introduced to modernise and make more transparent the activities and oversight of intelligence agencies.[14]

---

[9] See http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and

[10] *National intelligence authorities and surveillance in the EU: Fundamental rights, safeguards and remedies,* FRA, http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and

[11] The MAPPING acronym stands for “Managing Alternatives for Privacy, Property and Internet Governance”. This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345. More information can be found via https://mappingtheinternet.eu/.

[12] https://www.cia.gov/library/reports/Policy-and-Procedures-for-CIA-Signals-Intelligence-Activities.pdf

[13] http://www.globalsecurity.org/intell/library/policy/national/ppd-28_signals-intelligence-activities_140117.htm

[14] See, for example, the New Zealand Intelligence and Security Act 2017.

*Civil society and private initiatives*

Globally, civil society groups have raised concerns about the legal framework for privacy protection in relation to electronic communications. The 2014 Web Index concluded that 83% of countries had weak or inadequate privacy protections, including lack of transparency about the nature and extent of law enforcement and security agency surveillance and protection for electronic communications.[15] These concerns, among others, have resulted in numerous multi-stakeholder and civil society initiatives calling for digital rights charters, including the Internet Charter of Rights and Freedoms, a product of the United Nations mandated Internet Governance Forum.[16] Each of these initiatives has, to varying degrees of specificity, raised concerns about the activities of intelligence agencies and called for greater clarity about the duties of States in relation to these activities.[17] More recently, the Web Foundation, which supports the Web Index, called for a Magna Carta for the Internet which would seek to build global consensus on core principles for Internet related policy.[18]

The private sector has continued to raise concerns about their legal requirements in response to intelligence agencies requests and their obligations to take action in relation to cybersecurity threats. The private sector has supported other initiatives calling for new international agreements in this area. For example, in early 2017, MicroSoft Inc re-ignited debate about an international agreement that would bind governments, calling for a "Digital Geneva Convention" that would govern responses to nation state cybersecurity attacks on civilians in times of peace and establishing guidelines for the role of technology companies in response to such attacks.[19] This proposal included "a neutral digital Switzerland", and an independent organisation that spans the public and private sectors with the aim of protecting civilians from nation state attacks in times of peace, in a role analogous to that of the Red Cross.

*Emerging debate on new standards applicable to intelligence agencies' activities*

A new debate has emerged specifically focused on new principles that should apply specifically to intelligence agencies. Some of these new principles have developed through multi-stakeholder processes (such as the Tshwane Principles[20] and the International Principles on the Application of Human Rights to Communications Surveillance[21]). Others relate specifically to data protection authorities, such as the Amsterdam Declarations on, firstly Genetic and Health

---

[15] The Web Index (2014) http://thewebindex.org/report/#6.1_privacy_and_surveillance
[16] See, for example, The Dynamic Coalition on Internet Rights and Freedoms, www.intgovforum.org
[17] See, for example, Rodriguez K, "A Principled Fight Against Surveillance", *Global Society Information Watch*, (2014), Hivos and Association for Progressive Communications, 11.
[18] See: https://webwewant.org/news/category/internet-charters/
[19] Smith, B. "The need for a digital convention", Microsoft Inc, 14 February 2017. Available at: See also: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00001euw80bnrgexcs4mntuoy2nwn
[20] Open Justice Initiative, "The Global Principles on National Security and the Right to Information" Available at: https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles
[21] Available at: https://necessaryandproportionate.org/principles

Data, Challenges for Tomorrow and, secondly, Data protection oversight of security and intelligence.[22] Others are currently under discussion, as noted above.

The breadth and depth of these initiatives vary enormously, yet the main threads of these principles have some consistent elements. These include requirements for transparency, accountability, operation according to the rule of law (with a clear authorisation framework), proportionality, data retention and oversight of use, use of least intrusive means to gather information, adequate remedies, whistle-blower protections, impartiality, integrity of systems and clearer definition of national security to guide the scope of agencies' activities (for example to exclude the use of intelligence agencies to gather information to protect commercial interests).

**Challenges**

Data protection authorities face challenges in monitoring these developments and determining how best to respond. Some of the initiatives are impractical, others may be conceptually flawed or overly ambitious. The trend, however, is clear: the policy discourse on governments' access to communications networks and systems to acquire content and metadata of citizens of their own and other countries is growing, with diverse aspects of the topic being discussed and researched in an increasing range of international fora. A core aspect of this discourse is the legitimacy of State intelligence gathering activities as a means to fulfil their obligations to protect both national and domestic security concerns and protect their citizens.

One challenge also emerges from how this particular rights discourse is framed. For example, the 2017 SRP report refers to polarised views that have emerged between those who view "surveillance" of any kind by the State pejoratively and those in the intelligence communities who do not accept the legitimacy of the term "surveillance" as applied to their activities. They reject a framing which equates "retention of telecommunications data" or even "bulk collection" with "mass surveillance" or even "surveillance".

This makes it problematic for such agencies to engage in discussion of new international agreements which are predicated on an acceptance of such a description of their activities. At the same time, those who do not accept the legitimacy of intelligence agency activities are opposed to developments which might result in perceived concessions which would provide a lawful basis for such activities or which might be viewed as legitimising "surveillance".

Such a polemic leaves little room for the viewpoints of others, including those in developing countries. Such countries may have legitimate concerns about serious internal and border security issues, justifying, in their view, intelligence gathering activities. These same States may face strong public demand for the maintenance of law and order, and may also face international criticism for a failure to ensure security in their region.

Faced with these emerging issues, data protection authorities must consider how best to respond. With their experience and expertise in data regulation and the promotion and protection of the right to privacy in law enforcement and security contexts, our view is that data

[22] See: The role of Data Protection Authorities in a changing society, 2015, https://icdppc.org/wp-content/uploads/2015/02/Amsterdam-Declaration-.pdf

protection authorities have a unique and important contribution to make to this emerging area. Indeed, if new principles are to emerge, it is vital that data protection authorities participate in and help shape the discussion as to which principles should apply to the activities of intelligence agencies.

**Next Steps**

One consequence of the contemporary debate about the legitimacy of, and conditions under which, governments undertake interception of communications, be it voice, data or otherwise, is that there is growing consensus there should be some internationally agreed principles governing these activities. Such a set of principles would form the foundation for accountability for such activities.

A starting proposition for a set of principles could be that State action to gather intelligence to protect national security and the safety of individuals is legitimate so long as it is governed and conducted in a manner that accords with international standards.

**Conclusion**

There is a clear trend in calls for the creation of a new set of international principles to strengthen oversight of intelligence agencies and their information (including telecommunications information) gathering practices. There are challenges for data protection authorities in determining how best to respond and where best to engage.

We conclude, however, that data protection authorities have a unique and valuable contribution to make and that their expertise and experience would be a positive contribution to the development of new principles.

**Recommendations**

The working group recommends that data protection authorities within the limits of their competence:

(a) support initiatives to identify, develop and share best practice in governance and oversight of the activities of intelligence agencies;
(b) participate in the emerging debate about principles which should apply to the activities of intelligence agencies;
(c) when in engaging in that debate, draw upon and promote the following principles:

*Legitimacy*: All States are entitled to protect the national security of their citizens and where States employ intelligence agencies in this role, those agencies must carry out their activities in accordance with the rule of law.

*Rule of law*: Intelligence agencies must operate with a clear legal mandate and authorisation framework that includes respect for all human rights, protection of the right to privacy, impartiality and the right to an adequate remedy for actions taken by those agencies.

*Review*: Intelligence agencies must be subject to efficient *ex ante* authorisation and *ex post* review of their activities.

*Proportionality, necessity, and least intrusive means*: Intelligence agencies' powers to collect personal information must be limited to those necessary and by way of the least intrusive means of collection in order to achieve those lawful objectives.

*Data retention and use*: Data protection rules should apply to intelligence agencies' retention and use of personal information, including the rights of individuals to have data minimized, deleted and corrected. These rights should only be subject to such limitations in accordance with law as are necessary in a democratic society.

*Accountability and transparency*: Intelligence agencies should have clear, publicly available accountability processes (including judicial, executive and parliamentary accountability) and should produce periodic reports about their activities.

*Oversight*: Intelligence agencies' activities must be subject to effective and independent oversight.