"Better protecting individuals in the context of international data flows:

the need for democratic and effective oversight of intelligence services"

Joint statement by

Alessandra Pierucci, Chair of the Committee of Convention 108

and

Jean-Philippe Walter, Data Protection Commissioner

of the Council of Europe

Strasbourg, 7 September 2020

Years after the Snowden revelations brought to light the breadth of mass surveillance by public authorities, the digitisation of our societies has continued at a rapid pace, notably accelerated by the current health crisis which required many of us to work, learn and socialise at a distance.

Personal data is generated by each of our keyboard strikes, every movement made under the gaze of cameras and smartphones, any message sent, or picture taken. As our lives become increasingly digital, and online services internationally intertwined, our personal data flow across frontiers, regardless of national or regional borders, and our effective protection becomes difficult to secure.

Privacy and data protection are fundamental rights. They are essential to the effective functioning of democratic societies and have become even more essential in our digital era.

The right to privacy is universally recognised by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. At regional level, the Council of Europe recently celebrated the 70th anniversary of the European Convention on Human Rights, with its safeguards in Article 8 on the right to respect for private life. And more recently, the European Union (EU) has included privacy and data protection in its Charter of Fundamental Rights.

Those rights cannot be compromised: they can only be lawfully limited, under specific and strict conditions, as may for instance be the case when threats to national security exist, or as was the case more recently, to our health.

Such restrictions on our fundamental rights to privacy and data protection are narrowly circumscribed and a number of safeguards have to be observed for such interferences to be permissible and the essence of the fundamental rights and freedoms to be respected.

The Court of Justice of the European Union recalled recently the crucial importance, at international level, of appropriate safeguards, enforceable rights and effective legal remedies when personal data are being processed for the purposes of public security, defence and State security.

In its judgment "*Schrems II*" [1] of 16 July 2020, the Court reaffirmed that personal data transferred outside the EU must be afforded a level of protection essentially equivalent to that guaranteed within the EU by the General Data Protection Regulation (GDPR), read in the light of the Charter of Fundamental Rights.

The Court concluded this was not the case under the "Privacy Shield" agreed by the EU and government of the United States of America (US),[2] as the limitations on the protection of personal data transferred from the EU - arising from the domestic law of the US on the access and use of such data by US public authorities and law enforcement – were not "circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary."[3]

This decision has implications beyond EU-US data transfers and raises broader questions relating to international data transfers, providing yet another opportunity to strengthen the universal data protection framework and to address the need for a global legal instrument on intelligence services.

A global issue

Some influential voices have been calling, in the aftermath of the *Schrems II* decision, for a legally binding international agreement for the protection of privacy and personal data.

This instrument exists: it is Convention 108+.

[1] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Case C-311/18, "Schrems II").

[2] Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield, invalidated on 16 July 2020.

[3] CJEU, Press release 91/20 of 16 July 2020.

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (more commonly known as "Convention 108")[4] is the only legally binding multilateral instrument on the protection of privacy and personal data open to any country in the world.

Convention 108 was opened for signature in 1981 and has since influenced various international, regional (as for instance the EU) and national privacy laws. It currently has 55 States Parties[5] and its Committee counts over 25 observers, forming a global forum of over 70 countries from six continents working together on data protection.

Convention 108 has recently been modernised in order to adapt this landmark instrument to the new realities of an increasingly connected world, and to strengthen the effective implementation of the Convention. The Protocol[6] amending Convention 108 was opened for signature on 10 October 2018 in Strasbourg and has since been signed and ratified by numerous countries.[7]

Once it enters into force, the amending Protocol will deliver two essential objectives: facilitating data flows and respecting human rights and fundamental freedoms, including human integrity and dignity in the digital age.

Convention 108+ (Convention 108 as amended by the protocol) is set to become the international standard on privacy and data protection in the digital age, and represents a viable tool to facilitate international data transfers while guaranteeing an appropriate level of protection for people globally.

It is up to policy makers and governments around the world to seize the potential of that Convention.

The United Nations' Special Rapporteur on the right to privacy, Professor Joseph A. Cannataci, has already twice recommended[8] "to all UN Member States to accede to Convention 108+".

Aside from its global nature, two other important features of Convention 108+ are of particular relevance in the reflections following the *Schrems II* decision and its implications at international level.

[4] Text of the 1981 instrument available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[5] Full list of parties available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=64GsTZPR

[6] Amending Protocol, CETS No. 223, available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[7] To date: 36 signatures and six ratifications, full list available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.

[8] 2018 Annual Report on the Right to Privacy to the Assembly General (Report A/73/45712) and Annual Report of 1 March 2019 to the UN Human Rights Council (Report A/HRC/40/63).

Firstly, in the context of data transfers from the EU, and the need to effectively secure an adequate level of protection essentially equivalent to that ensured within the Union, it is important to recall that the GDPR in its recital 105 makes explicit reference to the Convention in the context of the adequacy regime. In deciding upon the level of data protection of the country seeking an adequacy decision, the third country's accession to the Convention should be taken into account. The relevance of the Convention in the context of an adequacy assessment is thus expressly acknowledged in the GDPR. Being Party to the Convention could in the future also facilitate the case-by-case assessment that companies are required to do in the context of standard contractual clauses[9], regarding the essentially equivalent level of protection to be guaranteed.

Secondly, regarding the specific issue of the processing of personal data for national security and defence purposes, Convention 108+ contains a robust system of checks and balances in its Article 11, complementing its fully horizontal scope of application (Article 3 of Convention 108+)[10].

The rights laid down in the Convention may only be limited when this is provided for by law and the restriction constitutes a necessary and proportionate measure in a democratic society on the basis of specified and limited grounds, including national security and defence.

Paragraph 3 of Article 11 specifically deals with processing activities for national security and defence purposes, and the requirement that such processing activities be subject to an independent and effective review and supervision is clearly laid down in the Convention.

While Convention 108+ provides a robust international legal framework for the protection of personal data, it does not fully and explicitly address some of the challenges posed in our digital era by unprecedented surveillance capacities. For years, calls[11] for a comprehensive international human rights law instrument framing the operations of intelligence services have intensified, and the need for strong safeguards at international level, complementing and specifying those of Convention 108+, can no longer be ignored.

---

[9] See paragraph 134 of the Schrems II decision.

[10] The Convention applies to all processing of personal data in the public and private sectors, including the security and intelligence services.

[11] Notably see:

- the 2013 Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=09000016805c8011 ,
- the Resolution 2045 (2015) on Mass surveillance of the Parliamentary Assembly of the Council of Europe (PACE) calling for a multilateral "intelligence codex": http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en
- the 2016 report to the Human Rights Council of the UN of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci: https://undocs.org/en/A/HRC/31/64
- the 2014 report to the General Assembly of the UN of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson: https://daccess-ods.un.org/TMP/5945256.35242462.html

A robust basis for future reflections

For over 60 years, the European Court of Human Rights has through its abundant case-law developed important safeguards for the protection of the right to privacy, as enshrined in Article 8 of the European Convention on Human Rights, including in a number of key cases regarding intelligence service large-scale monitoring of communications[12]. Article 13 on the right to an effective remedy is another crucial protection for the individual.

In order to determine whether interferences with the right to private life or correspondence is necessary in a democratic society, and a fair balance is struck between the different interests involved, the Court examines whether the interference is in accordance with the law, pursues a legitimate aim, and is necessary, and proportionate to the aim pursued. In so doing, it has developed precise safeguards and conditions that must be respected by intelligence services.

The exponential increase in trade and information exchanges that is witnessed in our digital era requires that stronger safeguards be guaranteed for personal data, wherever they flow, and wherever they end up. There is a strong need to tackle at international level the complex and sensitive question of the democratic and effective oversight of intelligence services.

The *Schrems II* decision touches upon two specific requirements: the need for legal remedies (i.e. effective and enforceable rights of individual redress, in front of an independent and impartial court)[13], and regarding the scale of certain surveillance programmes, the absence of limitations on the access by State authorities to personal data, thereby infringing the principle of strict necessity and subsequent proportionality of the restrictions to human rights[14].

The Court of Justice of the EU concluded "the law of that third country does not provide for the necessary limitations and safeguards with regard to the interferences authorised by its national legislation and does not ensure effective judicial protection against such interferences",[15] as it already did in its first decision "*Schrems I*"[16] invalidating the predecessor EU-US "Safe Harbour" agreement.

[12] See the Factsheet on Mass surveillance: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf and the case-law Research report on national security: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf

[13] See paragraphs 191 *et seq.* of the Schrems II decision.

[14] See paragraphs 179, 180, 183 to 185 of the Schrems II decision.

[15] See paragraph 168 of the Schrems II decision.

[16] Maximillian Schrems v. Data Protection Commissioner (Case C-362/14, "Schrems I").

At the level of the United Nations, Member States recalled in Resolution 68/167 on the right to privacy in the digital age[17] "that unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data, as highly intrusive acts, violate the rights to privacy and to freedom of expression and may contradict the tenets of a democratic society", and called upon all countries "to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law".

Creating such conditions implies today that countries must agree at international level on the extent to which the surveillance performed by intelligence services can be authorised, under which conditions and according to which safeguards, together with independent and effective oversight[18].

The case-law of the European Court of Human Rights has established that to be permissible, interference with the rights of individuals must meet a number of conditions and must notably be based on law (which means that the circumstances and conditions need to be defined by legal provisions, and the implications must be foreseeable for individuals), and must be proportionate and necessary in a democratic society. Individuals affected must have recourse to effective remedies:

> *"… in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse* (see *Klass and Others*, 1978, §§ 49-50). *This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law"*[19].

The time has come to use the numerous criteria developed by the Courts, including the US Supreme Court, in respect of what constitute adequate and effective guarantees, effective accountability, and independent oversight of intelligence services,[20] and find consensus on this critical issue at global level.

[17] Resolution available at https://undocs.org/A/RES/68/167

[18] See the Issue Paper 'democratic and effective oversight of national security services' published by the Council of Europe Commissioner for Human Rights, https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb

[19] Big Brother Watch and Others v. the United Kingdom, 13/09/2018, §18.

[20] Also see the research published by the European Union Agency for Fundamental Rights (FRA) on 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", volumes I and II.

An ideally placed forum

The Statute of the Council of Europe provides the necessary material and territorial scope of action needed for this important work.

It enables the Organisation to both work on global issues, with participation of all regions of the world (as is the case with Convention 108+ or the Budapest Convention on the fight against cybercrime which currently counts 65 Parties[21]), and to work on national security and defence matters, which are outside the jurisdiction of the European Union[22].

Extensive work on counter-terrorism has already been carried out by the Organisation. Bringing together under a single roof national security experts and data protection experts will not be difficult, as it has already been done with the law enforcement and data protection experts in the context of the work of the cybercrime committee.

This is a key moment for countries around the world to set a path for the next 70 years of protection of human rights. Recognising the vital importance of data protection and the significance of transborder data transfers in today's digital environment, they should accede to Convention 108+ and should also seize the unique potential offered by the Council of Europe, and the chance that is given to address the question of the operation of intelligence services, under the aegis of a globally respected human rights organisation.

Alessandra Pierucci and Jean-Philippe Walter

[21] Full list of parties available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LwuEXVvQ

[22] Article 4.2 of the Treaty on European Union.