Check against delivery

Statement by Joseph Cannataci

SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY

General Assembly
73rd session
Third Committee

26 October 2018

New York

Thank you Mr. Chair.

Distinguished Delegates, Observers, Ladies and Gentlemen:

It is an honour to present my third Annual Report to the United Nations General Assembly. My statement addresses key issues emerging internationally with regard to the right to privacy, and provides my final recommendations on Big Data – Open Data.

Privacy has never been more at the forefront of political, judicial or personal consciousness than now as the tensions between security, corporate business models and privacy continue to take centre stage.

The past year has been extremely productive – full of engagements with civil society, governments, law enforcement, intelligence services, data protection authorities, intelligence oversight authorities, academics, corporations and other stakeholders, which has forged directions and leadership for this important human right.

In March 2018 I presented to the Human Rights Council, a comprehensive review of my first three year term as inaugural Special Rapporteur on the Right to Privacy. The report provided an account of my activities in each of the mandate's areas.

It is a great honour to have had my term extended to 2021 and to continue this important work.

Security and Surveillance

Security and surveillance revelations led to the creation of the position of this position of Special Rapporteur on the Right to Privacy, and its appropriate therefore that I address this troubling issue early in my presentation.

After Edward Snowden revealed details of surveillance and intelligence sharing programs operated by the United States and the United Kingdom, applications were lodged with the European Court of Human Rights concerning the bulk interception of communications; intelligence sharing with foreign governments; and the obtaining of communications data from communications service providers under the United Kingdom Regulation of Investigatory Powers Act 2000.

The European Court recently found that bulk interception is not inherently incompatible with a human rights regime provided that the right safeguards are in place and that there is no other way in which the legitimate objectives could be reached. The Court further found that the regime for sharing intelligence with foreign governments did not violate Article 8 or 10 of the European

Convention of Human Rights, articles which closely mirror UN provisions. The European Court however found that the United Kingdom's bulk interception regime as operated to 2016 violated Article 8 and 10 of the European Convention on Human Rights on account of the inadequate safeguards it deployed.

While this judgement concerned the United Kingdom's earlier surveillance legislation, its findings are very significant. I bring them to the attention of Member States for consideration of their practices and frameworks.

I also want to bring to the attention of the General Assembly, the Australian Government's Telecommunications and Other Legislation Amendment (Assistance and Access) Bill which would have profound impacts on human rights and cybersecurity internationally and domestically should it eventually find its way onto the statute book.

I have made a submission to the Australian Parliament and to the Australian Government, and a public statement saying the Bill is fatally flawed, such are my concerns.

My concerns include:

- The Bill is a poorly conceived national security measure that is equally as likely to endanger security as not;

- It is technologically questionable if it can achieve its aims and avoid introducing vulnerabilities to the cybersecurity of all devices - irrespective of whether they are mobiles, tablets, watches, cars, CCTV, and, it unduly undermines human rights including the right to privacy.

- Assurances that it is not a 'backdoor' into encrypted communications are unreliable since it may create, in effect, additional keys to the front door, or even more front doors.

- The Bill has an overly high level of discretion on the use of exceptional powers. It lacks judicial oversight, or independent monitoring, it lacks transparency, and the proposal to introduce software into device(s) is disturbingly akin to government hacking.

- The Bill was introduced into Parliament after an inadequate period of consultation, reportedly over 14,000 submissions, and just two weeks after consultation close.

- My concerns are compounded by the Australian Government's stance on remedy for serious invasions of privacy and Australia's limited human rights and privacy protections. Unlike its neighbour New Zealand, its Privacy Act has failed European adequacy assessment.

An international approach to addressing the challenges posed by encryption for law enforcement and national security is required. All countries need an approach that avoids weakening encryption and destroying the national security of other countries.

I commend to Member States the approach of the Government of the Netherlands, which recognised that :

- national action cannot be seen separately from its international context, and
- the lack of options for weakening encryption products without compromising the security of digital systems that use encryption.

The International Intelligence Oversight Forum (IIOF) which I organise on an annual basis will meet in Malta in late November. Without a doubt, this Bill will be discussed. Interest is such that the Forum is over-subscribed.

Work of Thematic Taskforces

All of the Thematic Taskforces are progressing well.

I brought forward the commencement of the Taskforce examining the corporate sector's use of personal information in response to recent events, including the Cambridge Analytica breach, the introduction of legislation such as the US CLOUD Act 2018, the Australian Assistance and Access Bill 2018, and the Microsoft v US Government case previously before the US Supreme Court. All of which have a strong connection to security and surveillance.

The Taskforce's membership is drawn from large corporations leading the digital era and who are key players in promoting the protection of the right to privacy in the digital world.

Under the 'Better Understanding of Privacy' Taskforce I have initiated an online consultation on gender perspectives of the right to privacy in the digital era. I encourage Member States to participate.

I present the final report from the Big Data – Open Taskforce today.

Introduction of Privacy and Data Protection Laws Globally

2018 has seen new privacy and data protections coming into force or being considered around the world.

Worthy of particular mention is the law proposed for India following the Puttaswamy decision. In South America, in mid 2018, Brazil's Federal Senate approved a General Data Protection Law which will become effective in February 2020.

Within the European Union there has been the first major modernisation of its framework for protecting privacy and data protection in over 20 years. The most obvious symbol has been the General Data Protection Regulation coming into force on 25 May 2018.

At the wider regional level, it is encouraging to note the modernisation of Convention 108. This is an important milestone as this international treaty covers national security and has been ratified not just by more than 55 UN member states, but an increasing number of non-European states.

In the report I have outlined areas of future work and the planned production of reports to the Human Rights Council and the General Assembly.

I will finalise also the reports on the official visit to the United States and to France both due March 2019. I may also report on other issues for example on privacy and gender.

Big Data-Open Data Report

Data is and will remain a key economic asset, like capital and labour. Its integral dependency upon personal information demands an accommodation with requirements of the right to privacy and data protection laws. It is impossible to isolate economic and political drivers from the policies and practices surrounding Open Data.

I presented my interim report on Big Data – Open Data to the General Assembly in October 2017 and flagged that an international consultation would occur during 2018.

The consultation with individuals, civil society, private and public sectors occurred in Australia on 26 and 27 July 2018.

The consultation considered the limitations of deidentification for protecting unit level records. One example considered was the release online, in August 2016 of a large longitudinal dataset for a 10% sample of Australians who had claimed national health benefits. This affected around 2.9 million Australians' medical data comprising prescriptions, surgery episodes, tests and visits to general practitioners and specialists The dataset had been downloaded 1,500 times before being taken offline following reports that doctors' IDs could be easily decrypted, and later, that patients could be identified. The release by the government department was to facilitate greater use of health data for medical research.

The consultation has assisted me form the final recommendations. These are:

Key Big Data – Open Data Recommendations

1. Unless and until, it is possible to unambiguously determine if there is personal information within aggregated data, or that disaggregated data cannot be re-aggregated, then Open Data should not contain unit level records.

2. Work to create international standards for privacy preserving data sharing, and international standardisation activities must continue without delay, and be supported by Member States.

3. As an interim minimum response to agreeing to detailed privacy rules harmonised at the global level, ALL UN Member States be encouraged to ratify data protection Convention 108+ using CETS223 and implement the principles contained there through domestic law without undue delay, paying particular attention to immediately implementing those provisions requiring safeguards for personal data collected for surveillance and other national security purposes.

4. As a matter of alignment of best practices, when reviewing and updating their domestic law as part of the transposition of Convention 108+, Member States outside the EU be encouraged to, if at all possible also incorporate safeguards and remedies found in the GDPR but not mandatory under Convention 108+.

5. Governments and corporations recognise the sovereignty of indigenous peoples over data that are about them or collected from them, and which pertain to indigenous peoples, knowledge systems, customs or territories, by always including formalised indigenous developed principles, a focus on indigenous leadership and mechanisms of accountability.

6. Member States need to review the adequacy of all legal and policy frameworks on AI for the protection of freedom of expression and the right to privacy; to foster strong multidisciplinary collaboration, and to devise strategies to prevent negative impacts on the enjoyment of human rights e from algorithms, automated processing, machine learning and AI.

Other Mandate Activities

Consultations were again undertaken during 2018-19 with civil society, Governments, law enforcement, intelligence services, data protection authorities, intelligence oversight authorities, academics, corporations and other stakeholders.

Throughout the year letters were issued raising matters concerning practices that appeared to be inconsistent with the right to privacy.

In June 2018 I visited the United Kingdom of Great Britain and Northern Ireland. I will submit my final report to the March 2019 session of the Human Rights Council. My preliminary report noted significant improvements since 2015. I remain concerned however, about a range of matters.

The next official country visit is to the Federal Republic of Germany – I start that visit this Sunday. In 2019 I expect to be visiting South Korea and South America.

I have made many Informal Country Visits and participated in International Events over the year including Australia in mid 2018, the Czech Republic in November 2017; France in 2017; Brussels January 2018 Geneva February 2018; Ottawa February 2018; Malta February 2018; Macedonia, March 2018; Israel June 2018; Italy, and the United Kingdom September 2018.

Acknowledgements

I have been assisted by many individuals and organisation. These are too numerous to list but I thank the Office of the High Commissioner for Human Rights in Geneva, the University of Malta, and the University of Groningen, Netherlands, those within Australia who enabled the Big Data - Open Data consultation.

I particularly recognise the efforts and support of non-governmental organisations, individuals and the regulatory and professional bodies who have assisted the mandate. Finally, my thanks to Taskforce Chairs, members, interns, and volunteers.

I thank you for your attention.