Check against delivery

Statement by Mr. Joseph Cannataci
SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY

1 March 2019

Geneva

President,
Excellencies,
Distinguished Delegates,

Friends and colleagues from civil society and academia
Ladies and Gentlemen:

It is an honour to present to the Human Rights Council, my fourth Annual report.

In the time at my disposal, I will today be focussing on:

- intelligence oversight;
- the first report of the 'Privacy and Gender' project undertaken by the 'Privacy and Personality' Taskforce,
- the Health Data Taskforce report, and finally,
- describe 'privacy metrics' work.

My activities during 2018 have been outlined in the report provided. I will only mention in order to bring to your attention the very productive and successful consultation in Australia on Big Data – Open Data which importantly introduced new areas, such as Indigenous Data Sovereignty and which was presented in detail to the general Assembly last October 2018.

Official country visits have occurred to the United Kingdom of Great Britain and Northern Ireland in June 2018, and Germany in November 2018.

I urge all Members States to read the report and all the Annexes closely since, as ever, the 10,700 word-limit imposed on me for the main body of the report, cannot do justice to the extensive work carried out by the mandate throughout the last twelve months. Most of the Annexes are still work in progress and their contents are open to consultation and I will be deliberately referring to some dates for receipt of feedback during this opening statement.

Privacy in context

As I have emphasised in the past, there is much work to be done to protect the right to privacy, and a defensive posture is not sufficient.

We, Member States and institutions of the United Nations, need to actively entrench privacy as a standard in a democratic society.

As more and more research – and more scandals - come to light and public opinion becomes louder and stronger, it is clear that citizens, civil society, regulatory and professional bodies, and even some countries and companies, want privacy to be actively protected. Increasingly, it is genuinely recognised and valued, that the right to privacy is a key foundation underpinning democracy.

This is a particular theme in the 'Privacy and Personality' Taskforce, and I look forward to addressing the Council on this in greater depth.

Security and surveillance

The modernised Convention 108[1], a recent global initiative, has, at Article 11, a set of principles and safeguards which, unlike the GDPR which so many of you have already heard about, are applicable to activities undertaken for national security purposes.

- My 2018 report to the General Assembly recommended all UN Member States who have not yet done so, to adhere to Convention 108+.
- New technologies may be used to undermine social values such as democracy and individual freedoms. Hence impacts upon democracy are a key base metric against which privacy-intrusive measures need to be evaluated.
- Let me publicly ask a question which vexes every single intelligence oversight agency that I meet around the world. Let me therefore ask "What happens to personal data as wel as intelligence analysis containing personal information once shared by the intelligence service of one country, with another country? Are the data, and thus the privacy of the individuals concerned, protected to the same standards in the receiving State as in the transmitting State?"
- In November 2018, five oversight bodies, all parties to Convention 108, drew attention to the potential oversight gap of international data exchange by intelligence and security services.[2]
- The oversight of intelligence activities spurred my intervention in the proceedings of the European Data Protection Board when considering the adequacy of Japan's domestic law and safeguards.
- And during the official visit to Germany, good practices in the exercise of bulk powers were debated.

My recommendations in this area, about which I have consulted with participants of the International Intelligence Oversight Forum, an annual event established by my mandate in 2016 and which was hosted by the Parliament of Malta in November 2018**, include:**

1. The incorporation into the domestic legal system of UN Member States of Article 11 of Convention 108+ for the protection of the fundamental right to privacy.

[1] The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

[2] https://english.ctivd.nl/documents/publications/2018/11/14/index

2. The adoption of the principle *"If it's exchangeable, then it's oversightable*"[3] in relation to any personal information exchanged between intelligence services and law enforcement agencies within a country, and across borders;
3. Member States when contemplating the use of bulk surveillance, adopt to the greatest possible extent, the criteria and safeguards featured in recent 2018 judgements referred to in my report.
4. Member States carefully considering the compendium of good practices developed by the Stiftung neue verantwortung **(at Annex 5)**.

- **The detailed recommendations can be found in my report. I take this opportunity to thank the Government of Malta and in particular the Speaker of the Maltese Parliament, Dr. Angelo Farrugia, for assisting my mandate by hosting the 2018 edition of the International Intelligence Oversight Forum known also as IIOF.**

Privacy, technology and other human rights from a gender perspective

- This report presents the first results of the mandate's 2018 call for input on 'privacy and gender in the digital age'.
- This work, in addition to the other themes of the 'Privacy and Personality' Taskforce such as children's privacy, is also open to Member States' participation. States are asked to register their interest to contributing to such work by 31 March, 2019.
- **The full report, at Annex 2,** is a compilation of submissions received by the mandate and, save for the Recommendations, does not necessarily represent the views of its lead author, Dr Elizabeth Coombs, Chair, of the Taskforce 'Privacy and Personality', nor of myself as Special Rapporteur.
- It was reported that individuals' experience of digital technologies and privacy is affected by their gender, along with factors such as ethnicity, culture, race, age, social origin, wealth, economic self-sufficiency, education, legal and political frameworks.[4]

[3] Personal data is exchanged between intelligence agencies located in different states on a regular basis but it is not necessarily subject to oversight by the independent oversight agencies located in either the sending state or the receiving state. Moreover, certain legislations effectively prevent such oversight or even consultation about the matter between the independent oversight authorities in the sending and receiving states. States are encouraged to amend their laws to empower their independent oversight authorities to consult with other independent oversight authorities in other states, and follow up on all cases of data exchanged with another state, irrespective of whether they are located in the receiving or sending state, including both raw unprocessed personal data or personal data which is contained in analysis typified by intelligence product. Both types of personal data are exchanged by intelligence agencies and LEAS and both should be subject to independent oversight in both the sending and the receiving state.

[4] Privacy Commissioner of Canada, 2018, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

- Submissions recognized that digital technologies have enormous effect upon privacy by amplifying the positive and negative gender experiences of the non-digital world.
- Cyber-misogyny[5] and general cyber-abuse of individuals according to gender are enabled by new technologies[6] with infinitely far greater reach, durability, and impact than previously.
- Those most at risk were reported as being women, young girls, children, LGBTQI individuals and communities.[7]
- Reports of harm arising from gender-based infringements of privacy include serious, well-documented effects. Violence and even death were consequences reported in submissions.[8]
- Invasions of privacy according to gender, are not trivial matters either for individuals, communities or society.[9]
- Submissions indicated good practices[10] and are outlined in my report and Annex 2.

Conclusions:

1. Gender based breaches of privacy are a systemic form of denial of human rights; they are discriminatory in nature and frequently perpetuate unequal social, economic, cultural and political structures.
2. The right to privacy is critical for those who face inequality, discrimination or marginalisation based on their gender, sexual orientation, gender identity, sex characteristics or expression.
3. States, companies, religious bodies, civil society, professional organisations and individuals, all have important roles to play.
4. Addressing gender based incursions into privacy requires frameworks at international, regional and domestic levels, with gender as a key

---

[5] LEAF 2014, http://www.westcoastleaf.org/our-publications/cybermisogyny/

[6] Eastern European Coalition for LGBT+ Equality's submission, 'Gender Perspectives on Privacy in Eastern Partnership Countries and Russia', 2018; UCL and Privacy International, 'Gender and IoT', https://www.ucl.ac.uk/steapp/research/themes/digital-policy-laboratory/gender-and-iot

[7] Kazakhstan Feminist Initiative "Feminita", ODRI Intersectional rights, "Stimul" LGBT Group and Transgender Legal Defense Project (Russia), Richard Lusimbo, MPact Global Action for Gay Men's Health and Rights, Transgender Europe TGEU, Federatie van nederlandse verenigingen tot integratie van homoseksualiteit - COC Nederland, and the International Lesbian, Gay, Bisexual, Trans and Intersex Association ILGA Submission 2018.

[8] APC Submission, 2018, Pushkarn, N. and Ren,MM, Submission 2018, "*Online Reputation, What are they saying about me*?", **a Discussion Paper, Office of the Privacy Commissioner of Canada, January 2016: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/**; Case submissions to TGEU; and European Union Agency for Fundamental Rights, Violence against Women: an EU-wide survey. Main Results. 2015.

[9] AWAVA Submission, 2018.

[10] Joint CSO Submission 2018; AccessNow The gender of surveillance: how the world can work together for a safer internet, February, 2018 https://www.accessnow.org/gender-surveillance-world-can-work-together-safer-internet/

consideration in such frameworks - ‘one size fits all’ approaches to privacy are insufficient.

5. States need to actively advance gender-privacy.
6. Transparency and responsiveness are needed by companies.[11]

I thank the Chair of the mandate’s Task Force on Privacy and Personality, Dr Elizabeth Coombs, for her work and assistance in producing this report. **The full conclusions and recommendations are in Annexe 2**.

Privacy and health data

- This report reveals that, like the Gender work, there are major emerging issues.
- The Taskforce on Health Data that I established two years ago, has identified issues ranging from Indigenous Data Sovereignty; prisoner populations; forensic databases; health apps and wearables; 'Smart' implanted health devices/prostheses transmitting real life data, and artificial intelligence/machine learning, and automatic processing issues.
- I stress, as I did to the General Assembly in October last year, that “Sensitive, high-dimensional unit-record level data about individuals should not be published online or exchanged unless there is sound evidence that secure de-identification has occurred, and will be robust against future re-identification.”[12]
- I intend to provide guidance for regulating health-related data to:

1. serve as a common international baseline for minimum data protection standards for implementation at the domestic level; and

2. to be a reference point for the ongoing debate on how the right to privacy can be protected in the context of health data, and in conjunction with other human rights in a global context.

- **The draft guidance you will find at Annex 3** of my report is open to written comments which should reach my mandate by **11 May 2019.** This will be followed by a public stakeholder meeting in Strasbourg on 11-12 June this year to discuss the substance of the recommendations in the light of the feedback received. Member States are very strongly encouraged to participate by sending delegations to this public consultation on the topic of Privacy and Health Data and may register their interest by 11 May. I would like to take this opportunity to publicly thank the Council of Europe for assisting my

[11] Australian Competition and Consumer Commission, ‘Preliminary Report of Inquiry into Digital Platforms’, 2018.

[12] Special Rapporteur on the right to privacy, 2018 Annual Report to the UN General Assembly, Recommendation at 117(k), p21, A/73/45712.

mandate by hosting the public consultation meeting in its premises in Strasbourg,

- A final –or near-final recommendation produced after the public consultation in June is expected to be incorporated in my Annual Report to the General Assembly in October 2019.
- I also thank the Chairs of the Health data taskforce, formerly Dr Steve Steffenson MD and now Professor Nikolaus Forgo', the many taskforce members, the secretariat, especially Sean McLaughlan, and other team members for their work.

Privacy metrics

- I am also consulting on draft "Metrics For Privacy" as a standard tool for use during country visits.
- A very preliminary first draft is appended to this report **(Annex 4). Individuals, civil society and governments are invited to send their comments by 30 June 2019**.

Acknowledgements

- There are many organisations and individuals whose support I wish to acknowledge, however, there is not sufficient time. Therefore, I thank everyone in this one brief statement.
- I do however, acknowledge the support of the Office of the High Commissioner for Human Rights in Geneva. The assistance of UN staff is gratefully acknowledged.
- My brevity in no way reflects the depth of my appreciation.

Thank you.