Welcome to the 2019 International Conference Closed Session

41ST INTERNATIONAL CONFERENCE
OF DATA PROTECTION AND PRIVACY COMMISSIONERS

ICDPPC
International Conference of Data
Protection & Privacy Commissioners

#ICDPPC2019

university of groningen

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

AUSTRALIA
ECU UNIVERSITY
EDITH COWAN

L-Università
ta' Malta

Professor Joseph Cannataci
UN Special Rapporteur on the Right to Privacy

What has the UN SRP been doing?

Official Country visits

1. Germany – Nov 2018

2. Argentina – May 2019

3. Korea – July 2019

Unofficial Country visits

4. Ghana – June 2019

Priority themes

i. Security and Surveillance

ii. Big Data & Open Data

iii. Health Data

iv. Use of personal data by corporations

v. A better understanding of privacy: Gender & Privacy + Children & Privacy

The International Intelligence Oversight Forum 2019

Tuesday 08 October 2019 – Lancaster House – London, United Kingdom

Professor Joe Cannataci – UN Special Rapporteur on Privacy

UN SRP Task Forces (Working Groups)

Corporations' Use of Personal Data: Meets every six months

• March 2019 - Malta.

• September 2019 – Brussels focus: online protections for children.

• Next meeting Washington – 1-3 April 2020 – Children + Encryption

• Encryption – Major drive on combating backdoors/weakening

Health Data Privacy

• Draft Health Related Data Recommendation: UN HRC March 2019.

• On-line consultation Feb-May 2019

• Consultation in June 2019 hosted by Council of Europe

• Finalised Recommendation July 2019; Explanatory Memorandum

• Will present to UN General Assembly – New York – Tue 29 Oct 2019

Privacy and Personality
A Better Understanding of Privacy:

Privacy and Gender

- On-line consultation August 2018 - February 2019

- Preliminary report to UN HRC in March 2019

- Public consultation on gender perspectives of the right to privacy in **New York on 30-31 October 2019.**

- Report on Privacy and Gender to be presented to UN HRC on 28 Feb 2020

Privacy and Children

- Background research Feb-Oct 2019

- Participation in activities of Committee – UN Convention Rights of the Child

- On-line consultation March – May 2020

- Consultation Meeting – **Tunisia (late October or early November 2020)**

- Recommendations in Report to UN Human Rights Council – March 2021

Draft Recommendation on Health Related Data

- Health is the most important fundament of everybody's life. We all have very legitimate interests in our dignity and autonomy being protected by the highest available standards in health-data related scenarios.

- The relationship between a data subject as a patient and a healthcare professional is highly sensitive. Protection of patients (and their genetic relatives) has been subject to legal and ethical considerations and rules for centuries.

- Principles like medical professional confidentiality, the obligation to establish fully informed consent for treatment, proper documentation of treatment and free choice of treating physician, are some of the fundamental outcomes of centuries of thought on how best to protect the rights of patients.

- Every medical situation produces personal data important for treatment purposes which needs to be processed following the highest legal and ethical standards.

- Digitalisation is producing more and more medical data, which will be increasingly shared between healthcare professionals.

Draft Recommendation on Health Related Data

- Tensions between different stakeholders pose challenging legal and ethical issues.

- Data processed for health purposes is important for many other stakeholders and for many different purposes outside of health care purposes.

- First, the patient her/himself has a legitimate interest in controlling this data.

- Second, there are other stakeholders such as patients' relatives, institutions to which the patient has an obligation, and indirect stakeholders such as medical researchers and the general public.

Health Related Data Recommendation

- **The management of health-related data requires due consideration of the lawful, proportionate and necessary elements of these interests based on the current 'best of breed' data protection standards applied, also with due consideration of the rights and protections of :**

  - Indigenous peoples and indigenous data sovereignty
  - People living with Disabilities
  - Immigration
  - individuals in the care of the state

- Combined with an understanding of the intersectionality of factors that affect both health workers and data subjects alike.

'Privacy: A Gender Perspective'

- **Is Privacy enjoyed differently by different genders?** In a word, yes.

- Privacy is a right for all. Yet privacy is experienced differently according to gender, gender identity, sexual orientation and expression.

- Digital technologies have amplified positive and negative experiences of the non-digital world across cyberspace.

Gender Privacy: Positives and the Negatives

The Positives: Digital technologies enable users to connect, exercise human rights, find and create information, and engage with people and interests. Very important for trans people and communities.

Cyber benefits are affected by structural inequities and discriminatory gender norms that fall heavily upon women, non-binary gender and cis-normativity individuals, the poor, and minority, religious or cultural communities.

The Negatives: new technologies are used to target, harass, and worse, LGBTI individuals and communities, and other populations.

'Cyber-abuse' of non-binary genders have been enabled by new technologies with *infinitely far greater reach, durability and impact than previously.* Poor, and marginalized populations can be doubly, triply affected.

Conclusions

- Breaches of privacy based on gender, gender identity and expression are a systemic form of denying human rights, frequently reflecting and perpetuating unequal social, economic, cultural and political structures and norms.

- Privacy from a gender perspective raises issues of privacy as bodily autonomy.

- Consequences of privacy infringements based on gender, can be deleterious to society as a whole. For example, when young girls and women witnessing the attacks and humiliation of high profile women, 'opt out' of civic roles and public life.

SOME PRELIMINARY RECOMMENDATIONS

- UN bodies to: (a) integrate gender and privacy into their respective mandates.

- Member States to:
  - (c) assess their legal frameworks for prevention and punishment of gender based privacy breaches against relevant laws and treaties at global, regional and national levels to remove discrimination based on gender and build in protections against the same;
  - (d) adopt policies, legal and regulatory frameworks providing protection for secure digital communications including by promoting strong encryption and anonymity-enhancing tools, products and services
  - (f) Take all necessary legislative, administrative and other measures to prevent, investigate and punish gender based privacy breaches

SOME PRELIMINARY RECOMMENDATIONS Cont'd

- (o) implement Principle 6 Yogyakarta Principles+10

- (p) ensure requirements for individuals to provide information on their sex or gender are relevant, reasonable, necessary as required by law for legitimate purpose in the circumstances where this is sought; these requirements respect the right to self determination of gender; ensure changes of name or gender marker is not disclosed without the prior, free and informed of the person concerned unless ordered by a court.

- (q) take all necessary legislative, administrative and other measures to fully respect and legally recognise individuals self determined gender identity.

- (r) implement a comprehensive legislative system for recognising gender identity allowing transgender people to obtain legal recognition of their gender and to change their legal name and gender including on legal documents, through effective and efficient procedures.

university of groningen

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

AUSTRALIA
ECU
EDITH COWAN
UNIVERSITY

L-Università ta' Malta

SOME PRELIMINARY RECOMMENDATIONS Cont'd

- (y) implement data protection and security protocols for captured images, including Privacy Impact and Risk Assessment and governance protocols with embargoes on face surveillance or other algorithmic analysis without judicial permission and independent oversight.

- Corporations to:
  - (aa) apply the 'UN Guiding Principles on Business and Human Rights' including gender assessments; provide access to remedy.
  - (cc) respect and legally recognise self determined gender identity
  - (ee) engage more women and LGBTQI people in the design and regulation of digital technologies.
  - (ff) provide greater transparency of and access to data profiles, and monitor these for gender bias by eg, algorithmic auditing.
  - (ii) Limit data collection, restrict further data processing, prevent unnecessary access to and exploitation of data.
  - (jj) resist requests for user data that do not comply with human rights standards.

Some Things Remain the Same...........

- Privacy continues to be at the forefront of political, judicial or personal consciousness as the tensions between security, corporate business models and human rights, escalate:

- Controversies continue with Big Tech companies post Facebook - Cambridge Analytica

- EU General Data Protection Regulation (GDPR) implementation;

- growth in countries introducing data and privacy legislation; globalisation of C108+

- Increases in surveillance and security legislation

Some Things are Emerging………..

- The connection between privacy and freedom of expression and freedom of association:
  - Take down action on 'hate speech' and discussions around
  - Anti protest legislation
  - Civil awareness and action eg protestors I Hong Kong bringing down 'smart'/surveillance poles
- The responses of Big Tech companies to ongoing privacy concerns – August 2019 28 platform inquiries
- Identity – documentation; verification
- Technological 'solutionism' – useful but is it addressing the root cause?

Some particular issues to mention……….

- Introduction of national ID systems based on biometric data in countries without data protection laws – India and Kenya

- Predictive modeling in governmental programs leading to automated inequality

- Adequacy – more countries seeking a positive assessment

Thank you for your attention

Special Rapporteur on Right to Privacy (SRP):

- Professor Joe Cannataci: jcannataci@sec.research.um.edu.mt , j.a.cannataci@step-rug.nl

Office of High Commissioner of Human Rights:

- Ms Krystel Abi Habib: kabihabib@ohchr.org

SRP Thematic Taskforces contact point:

- Dr Elizabeth Coombs: ecoom02@sec.research.um.edu.mt