"Challenges in harnessing digital solutions to cope with the pandemic"

Wednesday 27th April 2022 – Virtually via Zoom

Professor Joe Cannataci

Chair in European Information Policy & Technology Law
Co-Founder STeP – Security, Technology & e-Privacy Research Group
Faculty of Law, University of Groningen, The Netherlands

Head of Department of Information Policy and Governance
Faculty of Media and Knowledge Sciences
University of Malta

Senior Fellow & Research Associate
Security, Intelligence & Defence Department – CNAM – Paris - France

university of groningen

le cnam

L-Università ta' Malta

United Nations A/76/220

General Assembly

Distr.: General
23 July 2021

Original: English

Seventy-sixth session
Item 75 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Right to privacy

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report prepared by the Special Rapporteur on the right to privacy, Joseph A. Cannataci, submitted in accordance with Human Rights Council resolution 28/16.

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci

Summary

In the present report, the Special Rapporteur on the right to privacy, Joseph A. Cannataci, aims to shed further light on how pandemics can be managed with respect to the right to privacy. It is a more definitive analysis building on the report of the Special Rapporteur to the General Assembly in 2020 (A/75/147) now that there is greater evidence available to allow a more accurate assessment of the ongoing coronavirus disease (COVID-19) pandemic. The Special Rapporteur examines in particular the impact of measures to combat COVID-19 on data protection, technology and surveillance and notes that ongoing measures taken by States to control the spread of COVID-19 continue to negatively impact the enjoyment of the right to privacy and personality and other interrelated human rights. The report contains recommendations to State and non-State actors for strengthening privacy and personality; safeguard children's access to online education; protect informational privacy; and ensure transparency and metrics.

Some key considerations

- We still do not have all the information required to make a definitive final assessment
- The Covid-19 pandemic is not yet over
- Governments are not necessarily keen to release full data about the pandemic in their country
- Governments do not wish to have their performance in handling COVID-19 subjected to scrutiny especially if they are close to elections…hence probably the reluctance to give us data

COVID led to privacy infringement

86. International treaties and most national constitutions allow States to temporarily increase their powers during a period of crisis, such as responding to the COVID-19 pandemic. The pandemic has intertwined health and surveillance and individual impacts. It thus requires management within the parameters established for these domains.

87. From a right to privacy perspective, the pandemic has enabled more intrusion by Governments and corporations into people's lives, infringing their right to privacy. While some infringements can be expected to arise during a pandemic, for public health purposes, it has, to date, proven to be impossible to gauge to what extent these have been necessary and proportional.

Shorcuts

89. The COVID-19 pandemic has seen shortcuts taken around the world in implementing national public health strategies. Some Governments have made use of emergency laws to pass mandatory contact tracing initiatives; others have taken advantage of the lack of robust national-level data protection laws to quickly roll out solutions such as contact tracing and registration of vaccinated individuals without paying heed to the right to privacy, or other human rights. Crisis responses, some of the "knee-jerk" variety, have included the exploitation of emergency laws and weak or non-existent data protection laws. Looming elections appear to have been, and continue to be, important factors for a number of States and Governments. [61]

The power of Apple and Google

91. In this context, countries were ill-prepared for the exertion of the independence and power of technology companies, such as the stance of Apple and Google on privacy for contact tracing app users. At the same time, it is important to acknowledge that these two companies appear to have been reasonably privacy-protective in their approach, in some cases possibly more so than some of the States which were keen to use the data they collected.

Compulsory use of apps …and voluntary

94. The privacy implications of compulsory contact tracing apps are obvious – consent and the ability to withdraw it have been recognized at law as integral parts of the right to privacy in many – although not all – cases. Compulsory measures also raise the risks of Governments and corporations misusing the sensitive data collected for the purpose of combating the pandemic through either "surveillance creep" or the repurposing of data without the users having any ability to have their data removed from databases. Voluntary contact tracing apps have suffered from low uptake, typically due to the lack of public trust in the Government's ability to keep their data safe and protected.

Necessary and proportionate?

95. There are also multiple implementation issues with the technology, including the lack of data showing the accuracy of some technologies. Most of the measures discussed collect a lot of sensitive data and it is difficult to estimate whether this collection is proportionate. While technology plays a critical role in the pandemic, it may also normalize surveillance in the future. Intensive and omnipresent technological surveillance is not the panacea for pandemic situations such as COVID-19.

UN SRP - Recommendations - 1

Privacy and personality

101. **States and non-State Parties should implement the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework with the gender guidance thereon (A/HRC/41/43, annex).**

102. **Adopt the recommendations of the Special Rapporteur on the right to privacy for protecting against gender-based privacy infringements (A/HRC/43/52, paras. 33 and 34).**

103. **Encourage partnerships with civil society and industry to co-create strategies and technological responses.**

104. **Involve groups in the community at particular risk in consultations on specific public health measures.**

105. **Reduce pandemic response infringements of privacy based on gender by requiring gender-aware privacy human rights impact assessments before introducing measures, strategies and legislation.**

106. **Regularly evaluate the effectiveness of the measures taken to include those in vulnerable and marginalized situations in response and recovery efforts.**

UN SRP - Recommendations 2

Informational privacy

111. Build human rights into the design, development and deployment of technological approaches to the pandemic.

112. Legislative protections based on common principles with guidance for specific situations are needed for all types of pandemic health measures. The Special Rapporteur recommends the use of the 11 common principles[64] for centralized and decentralized public health surveillance systems, legislative measures for communicable diseases and their utilization when assessing pandemic prevention policies across the world:

(a) Establish "privacy by design" and "by default" from the outset by incorporating an overarching human rights assessment alongside a data protection assessment for public health measures with a special focus on epidemics and pandemics;[65]

(b) Privacy should be considered from the very beginning of the response to any epidemic or pandemic. Indeed, it should be a cornerstone of any national strategy on how to deal with an epidemic, well thought out, years in advance as an integral – and well-integrated – part of the overarching human rights assessment mentioned above;

UN SRP Recommendations 3

(c) Insert clear and detailed controls in the region's or individual country's data privacy law;

(d) To provide the necessary clarity and legal foundation more effectively than by delegated acts or regulations, and achieve greater uniformity in the jurisdiction;

(e) Guarantee access to sites, events, facilities, education, etc., to avoid discrimination;

(f) It is vital to protect vulnerable groups adversely and differentially impacted by pandemic surveillance measures;

(g) Minimize and define authorized uses of COVID data to ensure that COVID-19 data is not used for other purposes once collected;

(h) Establish "purpose specification" as in many existing data protection laws;

(i) Minimize data collection;

UN SRP Recommendations 4

(j) **To ensure that data collection measures are proportionate, establish a generally accepted risk management approach and assist in limiting the damage caused by data breaches, cyber incidents and function creep;**

(k) **Anti-coercion provisions: the requirement to use or show proof of use should be prevented or strictly defined and contained by legislation. Other demands or requests to see certificates of use should be prevented by defining such behaviour as an offence under the law. Enforcement is needed, as are remedies;**

(l) **Prevent "surveillance creep": avoid following the example set by Singapore, which in 2020 promised "tracing only"; then reneged in 2021, allowing criminal investigations;**

(m) **The voluntary participation required by most pandemic prevention measures needs public trust to work. Future expansion as a surveillance measure to other areas for example, criminal investigations, must be made unlawful for this trust to exist;**

(n) **Continuous deletion programme (if data is collected): the legislation itself should require continuous deletion of any collected data within a short period of time, such as the individual's infectious period or some other evidence/scientifically based time period;**

UN SRP Recommendations 5

(o) **"Sunset clause" for whole system and mandatory, independent "audit of closure" of all epidemic data systems must be entrenched in law and strictly enforced: establish a fixed period or independent assessment of necessity to ensure that pandemic surveillance systems are shut down, with a statutory based requirement for independent audit that this has occurred;**

(p) **Supervision and periodic public reporting by independent data protection authority: supervision of these surveillance systems must be external and independent;**

(q) **Transparency: the necessary conditions should be identified in consultation with experts and civil society. It may take the form of releasing any source code used to build surveillance systems (such as contact tracing apps), conducting comprehensive data protection impact assessments and releasing data on the effectiveness of techniques used for pandemic surveillance.**

113. **An ongoing dialogue with the big tech companies should complement formal and informal public debate of the roles and responsibilities of big tech companies in carrying out a privacy-protective role in pandemics.**

UN SRP - Recommendations 6

Transparency and metrics

114. **Health emergency powers require assessment for their necessity and proportionality. As part of this periodic and regular assessment:**

(a) **The Special Rapporteur on the right to privacy, alone, as well as together with other mandate holders, should revisit the situation regarding notifiable and communicable diseases with a special focus on COVID-19, but not limited to COVID-19, at a minimum every 24 to 36 months in order to identify existing and emerging risks, as well as understand the most effective and privacy-friendly policy initiatives that can be used to prepare for pandemics within a holistic approach to human rights protection;**

(b) **If a State decides that technological surveillance is necessary as a response to the global COVID-19 pandemic, it must prove both the necessity and proportionality of the specific measure and establish a law that explicitly**

UN SRP Recommendation 7

provides for such surveillance measures containing mandatory explicit and specific safeguards;

(c) States and corporations should build human rights into the design, development and deployment of technological approaches to the pandemic, given the enormous implications of digital technologies for a broad range of rights, particularly privacy;[66]

(d) States and corporations should adopt user-centric, rights-respecting technological design whereby, for example, in the case of "vaccine passports", travellers can carry their data themselves for presentation upon request;

(e) External review of States' pandemic responses is required, and States' pandemic management should be assessed, together with other internal human rights responsibilities in their regular periodic reviews at the United Nations level.

LexConverge

Law ▸ Across Disciplines ▸ Across Technologies ▸ Across Cultures

Thank you for your attention

E-Mail: jcannataci@sec.research.um.edu.mt

Web: https://www.rug.nl/staff/j.a.cannataci/cv

https://www.um.edu.mt/maks/ipg/staff/josephcannataci

https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/JoeCannataci.aspx

university of groningen

le cnam

L-Università ta' Malta