Annex 4: Privacy Metrics - Consultation Draft

'Metrics for Privacy - A Starting Point',

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

Background:

This document is Version 0.1 (as at 13 February 2019). It is emphasised that this document is very much work-in-progress and is known to be incomplete. Starting from the Thematic Action Stream of Security and Surveillance, and using questions asked during 2017-2018 to national authorities, civil society and other stakeholders during country visits to USA, France, UK and Germany, a list of areas that may indicate the state of privacy within a country, has been compiled. There are additional questions included which extend beyond Security and Surveillance which will be updated when further comments are received about the mandate's work on Big Data and Open Data, Health Data and Privacy and Gender.

Scoring systems/weighting are still subject to consideration as these are especially debatable.

This very early version of the document is being released for consultation as a 'thought starter' in order to provide the opportunity for comment and contribute to this work and its development.

Individuals, civil society and governments are invited to send their comments and suggestions by 30th June 2019.

Draft Questions:

1. Does your country's constitution have a provision which specifically protects privacy or which has been interpreted to encompass a protection to privacy (+5)?
2. Does your country's constitution extend privacy protections beyond the standards set in Art 12 UNDHR, Art 17 ICCPR, ECHR Art 8? (range of +1 to +5)
3. Does your country have a constitutional provision and/or constitutional jurisprudence which recognises the right to free development of personality (+5) and/or autonomy of thought and action of the individual (+5)?
4. Does your country have jurisprudence, especially from its highest court, which significantly reinforces the right to privacy? (e.g. right to personality, informational self-determination, digital privacy, requirement for judicial warrant to search cell-phone, requirement for judicial warrant to plant tracking device etc.), (range +5 to +20)
5. Does your country belong to a regional grouping wherein the citizens of your country can appeal to a regional court which has the power to over-ride decisions by your own country's highest court thus adding a potential additional layer of safeguards for privacy protection (+10)
6. Does your country have, in addition to any possible constitutional and supra-national protection, one or more specific privacy laws of any sort? (+5)
7. Does your country's privacy law meet Convention 108+ standards (+20)?
8. Does your country's privacy law go beyond Convention 108+ standards to GDPR standards (+5)
9. Does your country have independent *ex ante* authorisation of surveillance? (+10)
10. Does your country have independent *ex post* inspection/oversight of surveillance? (+10 if fully independent of *ex ante* authorisation or +5 if part of *ex ante* authorisation authority)
11. Does your country have an independent *ex ante* and *ex post* surveillance authorisation which is on a full-time basis (+5) and which is properly resourced with adequate quantity (+5) and quality (+5) of human resources required to carry out the tasks it is expected to do?
12. Does your country allow politicians in power (the Executive branch of Government) to be involved in the decision-making authorising surveillance and, if yes, is their's the only authorisation required (-30) or is it held in check by independent judicial review (+15)?

13. Does your country's independent oversight authority have technical systems in place such as a secure room with direct access to the IT systems of Law Enforcement Agencies (LEAs) and Security and Intelligence Services (SIS) from which independent external oversight can be exercised at will without prior notice being given to the LEA or SIS concerned (+10)?
14. Does your country have Parliamentary (Legislative branch of government) oversight (+10) of any surveillance which is authorised by either the Executive branch and/or the Judicial Branch of Government and which has the power to change the behaviour of LEAs and/or SIS carrying out surveillance?
15. Does your country have independent Judicial (Judicial branch of Government) oversight (+10) of the activities of LEAs and/or SIS or are any of their activities precluded from judicial oversight by any law (-15)?
16. If your country's judges are involved in the oversight of surveillance, have they received specific training about surveillance and related law enforcement and intelligence activities? (+5)
17. If your country has mechanisms for the oversight of surveillance activities, irrespective of whether the surveillance is carried out by LEAs or SIS, do these independent oversight authorities have an exclusively advisory status (+5) or do they have the power *de jure* (+5) and/or *de facto* (+10) to impose changes and sanctions on the related activities of the LEAs or SIS?
18. Does your country share personal information and/or intelligence product with other countries and, if so, does it have adequate privacy safeguards in place for those occasions where such sharing of information/intelligence product occurs? (+5)
19. Does your country have technical capabilities for bulk powers (-55) and, if so, does it have a law granting a legal basis for bulk powers (+20) and detailed adequate safeguards for the use of bulk powers (range of +1 to +35)
20. Does your country systematically monitor private communications within its borders (-55) and, if so, do such means of monitoring communications require their source code to be approved by a control authority which possesses the required technical and legal expertise and all of this within a range of detailed privacy safeguards (range of +1 to +55)?
21. Does your country have an agency devising and enforcing standards of encryption which may possibly enhance privacy? (+10)
22. Does your country require corporations to weaken encryption (-20) in communication technologies?
23. Does your country carry out intensive policing of the internet as used by your country's citizens and residents, monitoring chat rooms and/or private correspondence and/or public correspondence/expression by citizens for conformity with political ideology or religious faith? (range of -1 to -55)
24. Does your country permit the profiling of individuals using financial credit scoring or other means which are not strictly subject to rigorous data protection laws (range of -1 to -25) and/or maintain a social credit scoring system utilising Big Data analytics to aggregate date from various sources including financial information, on-line behaviour, etc. in order to create a profile of an individual? (range of -1 to -50),
25. Does your country permit unfettered export (-10) and import (-10) of surveillance technologies?
26. Does your country have laws negatively affecting the privacy of minorities such as sex workers (-10)?
27. Does your country have any other laws or policies not contemplated in the above questions which negatively impinge upon (range of -1 to --20)) or positively contribute to the protection of privacy (range of +1 to +20?
28. Does your country have a police and/or intelligence service which systematically profiles and maintains surveillance on large segments of the population in a manner comparable to that of the STASI in the 1955-1990 GDR? If yes, then this is a "failing subject" (say. -1,000 – subtract one thousand marks) so please abolish that system and THEN start again at 1-27.