Submission # 72

Name: Joe Cannataci

Organization: University of Groningen

How would you define the stakeholder community or communities to which you belong?

Academic

Are there any suggestions that you wish to make in respect of the proposed themes, questions and indicators which are included in the framework as it stands?

1.1 Paragraph E1 poses the question “Is the right to privacy guaranteed in law and respected in practice”. The suggested indicator is “constitutional or legal definition of privacy and right to privacy”. This indicator goes to the legal nature of privacy in a jurisdiction only. It does not address ‘practices’. The indicator must also account for practical aspects of the implementation of this right.
It will also be necessary to consider other laws within the jurisdiction that might be inconsistent with the right to privacy in practice.
s1.2 Further, under Category R – Rights, Theme A to assist achieve the aim of identifying gaps within a country, reference to the existence of a hierarchy of law, policy and practices at international, regional and national levels would be a constructive addition. An indicator which asks ‘Has there been an assessment of the hierarchy of relevant laws at global, regional and national levels, that facilitates appreciation of the gaps in our framework in relation to Internet Universality?’
This issue is also applicable to Theme E – Privacy.

Are there any suggestions that you wish to make in respect of the proposed themes, questions and indicators which are included in the framework as it stands?

2.1 The recitation of themes in Category R refers to some rights as rights, but other rights are not referred to in this manner. This will confuse readers and not facilitate the appropriate understanding of human rights . An example is Theme C, “the right to access information”. However, Theme E is described as “Issues relating to privacy”. Each of these rights, and other rights also not described as rights, need to be referred to as rights to ensure that they are equally represented in the document. In addition, currently the recitation of these rights leads to the inaccurate conclusion that the right to privacy is the only area where issues arise. I recommend amending Theme E (and any other themes not identified as rights) to “Theme E is concerned with the right to privacy”.
2.2 The recitation under the Theme E heading on page 10 of the document refers to Article 12 of the UDHR and Article 17 of ICCPR. However, the reference

made omits a key aspect of the right to privacy in both these documents. That is the reference to attacks on reputation and honor in both articles, and to the protection of law against such attacks. The internet is an enabler of attacks on reputation and honor and these indicators are inaccurate in summarising the relevance of both these articles to the issues at hand, and do not appear to align with references to “recourse” and “redress” made in following paragraphs.5 Recommendation: to support these references, the additional aspects of Articles 12 and 17 are included in the recitation.

Paragraph E6 seems to bear some relation to the aspects of Articles 12 and 17 in so far as they relate to redress. It is pleasing to see this included in the indicators, however enforcement is important here, specifically what mechanisms exist to correct online information, or take it down, or enforcement/implementation of the right to be forgotten in jurisdictions.

2.3 Paragraph E2 refers solely to “redress”, whereas following bullet points refer to “recourse and redress”. Should these be made consistent with each other, and is the addition of “recourse” in bullet points intended to cover something additional to “redress”?

2.4 Paragraph E2 refers to an independent Data Protection Authority and while it appears this is being used in a generic sense, that is, where any independent entity charged with protecting privacy is intended to be covered. A better option is dispense with specific wording concerning the nature of the entity, and utilise some generic wording identifying the purpose of the entity that is related to this section. An example might be “existence of an independent entity responsible for privacy rights and/or data protection and/or information security”. Security of information is not all that the right to privacy involves and additional aspects of the right to privacy need to be included in this indicator.

2.5 Paragraph E5 relates to surveillance. Please find attached a copy of the Legal Instrument recently published concerning surveillance. I believe that it has a bearing on this section, and surveillance referred to generally in the document. With regard to the specific wording of the first bullet point, limiting this to surveillance might be too narrow. The mandatory data retention scheme in Australia, for example, might not be part of the “legal framework for surveillance” but could be used for this purpose and requires the storage of significant data about internet users. Law Enforcement Agencies (LEAs) may have access to that material in certain circumstances, but LEAs do not store or collect it, rather other entities are co-opted to collect and store it. This is an example of the kind of issue that the indicators should be developed to include to ensure accuracy.

2.6 Paragraph E4 concerns the registration requirements for accessing the internet. Care is needed to ensure this indicator is broad enough to cover both ISP and mobile phone access to the internet. Therefore, identification and registration requirements for SIM cards etc... should also be considered, as well as other devices for accessing the internet.

2.7 With regard to paragraph E5, it is pleasing the see the distinction between the legal framework and the practical operation (as is the case for paragraph E3)

5 See paragraphs E2, and bullet points 1 and 2 of paragraph E2.

being recognised. A good example might be legislation that excludes Small and Medium Enterprises (SMEs) as such exemptions render such legal frameworks significantly less powerful than they might appear at first instance.

2.8 The indicator for paragraph E7 will need to be developed to ensure that the necessity, proportionality and transparency of requirements for internet businesses to provide information to government agencies is included in the indicator. An assessment of these matters will need to be made and in the interests of clarity, this ought to be included in the indicator itself.

2.9 Paragraphs in section D3 and 4, as well as paragraphs E1, E3 and E5 relate to sharing and use of data. These sections need clarity clarity to record that open

data should not include personal data. Granted there are some exceptions where personal data might be able to shared, however generally this would not include Open Data. Care is needed to ensure that any reliance of de-identified data or anonymised data is undertaken effectively and be cognisant of the current concern that other available data sets can be used to identify data sets thought to be anonymous or de-identified.
Pargraph E5 is of particular concern as it appears to suggest that data should be shared without restrictions, however this is not consistant with the right to privacy as a number of restrictions may be required (such as the exclusion of personal data). It may very well also be inconsistant with other rights in this document. I recommend that you include a reference such as “without any restrictions other than those required to give effect to the rights of individuals”.
The recital under Theme E in this document recognises this aspect, and needs extension to other sections of the document and other rights. It is pleasing to see the right to privacy recognised in this way.
2.10 With regard to paragraph D4 first, it would be better expressed as two separate questions or issues. Currently two issues are conflated but which are not compatible and effectively now suggest that businesses have privacy rights.
Recommendation: consider reframing the questions as:
Are citizens taking action to reduce risks to their privacy rights and security online.
Are business taking action reduce risks to the security of the information they hold, and the privacy obligations they have to individuals.
The indicators arising from paragraph D4 relates solely to information security, and privacy does not seem to be reflected other than as a consequence of being related to security. While related to privacy, information security is not the same thing as privacy rights. Privacy rights are much broader and need to be reflected in these indicators separately.
While individuals and businesses are mentioned in this paragraph, there is no mention made of analysing or measuring government information security (or privacy) practices and the practical implementation of privacy rights connected with this issue. The indicator could be much more meaningful with the inclusion of the government as an entity to be assessed. An additional question is needed to ensure equal coverage of individuals, the private sector and the public sector.

What sources and means of verification would you recommend, from your experience, in relation to any of the questions and indicators that have been proposed?

Legislation and policies, regulations, rule, codes etc need to be considered. There are a number of additional issues that require consideration here which would be better undertaken through discussion.
Category R: Rights
This category of the indicator framework is divided into six themes:
• Theme A is concerned with the overall policy, legal and regulatory framework for human rights and their relation to the Internet.
• Theme B is concerned with freedom of expression.
• Theme C is concerned with the right to access information.
• Theme D is concerned with freedom of association and with rights to participate in public life.
• Theme E is concerned with issues relating to privacy. Issues with the placement in the hierarchy and this wording have been addressed above.
• Theme F is concerned with economic, social and cultural rights.
THEME E – PRIVACY

Article 12 of the UDHR and Article 17 of the ICCPR are concerned with privacy. Article 17 of the ICCPR provides that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.' Regional rights agreements also address issues of privacy in their regions. The UN General Assembly has adopted a number of resolutions concerning 'the right to privacy in the digital age,' which, in addition to general principles, have addressed issues including surveillance, encryption and anonymity.
See above comments in relation to 'reputation and honour'. And in relation to the international hierarchy of laws for the protection of privacy expressed in the covering correspondence and under Theme A.
E.1 Is the right to privacy guaranteed in law and respected in practice?
Indicator:
• Constitutional or legal definition of privacy and right to privacy
E.2 Is the protection of personal data guaranteed in law and enforced in practice, with respect to governments, businesses and other organisations, including rights of access to information held and to redress?
Comment: Redress, in some jurisdictions, includes the ability to have personal information corrected. Point may be repeated for following bullet points that refer to redress. Why does "recourse" appear in some of these sentences and not others? What, specifically will be looked for? Evidence of implementation of the right to be forgotten?
Indicators:
• Existence of a legal framework for data protection, including monitoring mechanisms and
means of recourse and redress, and evidence that it is respected and enforced by government
• Existence of legal framework governing commercial use of personal data and international
data transfer, including monitoring mechanisms and means of recourse and redress
Comment: Specific attention needs to be given to the application of laws to various sectors of the country. For example, there may be a privacy law that applies in the jurisdiction, however if most of the private sector is excluded because it does not apply to SMEs, this needs to be reflected in the metric applied here.
• Existence of an independent data protection authority
Comment: Data Protection, Privacy and Security of Data are not interchangeable terms and as this is the privacy section, more specificity is warranted. Consider also noting the need for adequate resourcing to be added here.
E.3 Are the powers of law enforcement and other agencies for the surveillance of Internet users necessary, proportionate and limited to circumstances which are consistent with international rights agreements?
Indicator:
• Legal framework for surveillance, and evidence concerning implementation
Comment: Limiting this to surveillance might be too narrow. See above comments in relation to the mandatory data retention scheme by way of example.
E.4 Are any requirements for identification and registration, including communications
registration, necessary, proportionate and consistent with international rights agreements?
Indicator:
• Existence and nature of identity and registration requirements, including verification processes
Comment: Will need to be broad enough to cover both ISP and mobile phone access to the internet and therefore identification and registration requirements for SIM cards etc...
E.5 Are data encryption and online anonymity protected in law and practice in a way that is consistent with international rights agreements?
Indicator:

• Existence of a legal framework consistent with international rights agreements and evidence that it is respected by government.
Comment: Note application point above where omission of, say, SMEs might render such legal frameworks significantly less powerful than they might appear.
E.6 Do citizens have legal rights to protect their online identity and to manage or correct
information concerning them online, in ways that protect both privacy and freedom of
expression?
Comment: Note the above point about 'reputation' in the UDHR and ICCPR.
Indicator:
• Legal frameworks and jurisprudence concerning privacy and freedom of expression
Comment: Privacy should be identified as a human right here. Enforcement needs to be considered that is, , what mechanisms exist to correct online information, or take it down or enforcement of the right to be forgotten.
E.7 Are government requirements for Internet businesses to provide information to government agencies concerning Internet users necessary, proportionate, transparent and consistent with international rights agreements?
Comment: Does 'government agencies' include LEAs and SIS?
Indicator:
• Existence and nature of legal framework and evidence that it is respected by government
THEME D – OPEN CONTENT
The theme of open content is concerned with providing for the availability of content of all kinds, including public information and information from other sources within and beyond the country, which can be made available online. Open content approaches seek to maximise the availability of content to end-users, through open licensing arrangements, without infringing international intellectual property agreements.
D.1 Does the government actively promote access to knowledge through its policies for education, culture and science?
Indicator:
• Existence and nature of government policy and practice on access to knowledge
D.2 Do arrangements for intellectual property protection balance the interests of copyright holders and information users in ways that promote innovation and creativity?
Indicators:
• Nature of the legal arrangements for copyright enforcement
Comment: Mandatory data retention regime would seem to require consideration here, without necessarily being "copyright enforcement".
• Government adoption of creative commons and other open access forms of intellectual property
D.3 Does the government provide or encourage access to and facilitate sharing of public
information?
Comment: This section should consider that "public data" that is being shared does not include "personal information or data etc..". It is consistent with privacy requirements that individuals cannot be identified in information shared openly, or in combination with other data sets.
Indicators:
• Existence and nature of government policies on access to and sharing of public information, including availability of creative commons or comparable licences
• Consideration should be given and cross-reference made to data/evidence for indicators concerning government policies on e-government and e-participation (Category R: Questions D.3, D.4) and public access facilities which can be used to access public information (Category A:Question A.5)

D.4 Does the government encourage the use of open educational resources (OER) and facilitate open access to academic resources?
Indicators:
• Educational policy framework concerning OER
• Arrangements for access to academic and scientific resources by higher education institutions and students
Comment: Subject to compliance with rights to privacy in any such information.
D.5 Does the government require ISPs to manage network traffic in a way that is transparent, evenly applied and does not discriminate against particular types of content or content from particular sources?
Indicator:
• Regulatory arrangements concerning net neutrality
D.6 Does the government allow citizens to publish and access content through protocols and tools of their own choice, including virtual private networks (VPNs)?
Indicator:
• Legal framework and practice concerning the rights of end-users to access content through all available tools, including VPNs
Category O: Openness
THEME E – OPEN DATA
Open data policies are concerned with making publicly available data that are gathered by governments (and, sometimes, other stakeholders) so that they can be used by any stakeholder. Data protection arrangements are important in ensuring that open data sets do not undermine individual privacy rights.
Comment: Consideration of the structural organisational arrangements is warranted here – for example, the conflict of interest that arises when an Information Commissioner with responsibility for privacy is also an Open Data Advocate? Do these powers need to be managed separately?
In relation to the statement “Data protection arrangements are important in ensuring that open data sets do not undermine individual privacy rights.”, this is important, but it is noticeable that the themes do not reflect any content related to the statement - with the possible exception of E1 bullet point 1. It is also a question of whether “Data Protection Arrangements” adequately covers the privacy rights of individuals. Currently it appears more data based, as in security of information, and not picking up the issues of the protection of the rights of an individual. There is also no reference to independence and adequate resourcing here.
E.1 Has legislation been enacted which requires open access to public data, and is that legislation implemented?
Indicators:
• Existence of a legal framework for access to open data which is consistent with international norms and privacy requirements
Comment: Consider that some jurisdictions have policies that exclude ‘personal data’ from ‘open data’ as a way in which to reduce violations of privacy requirements.
• Evidence concerning the extent to which open data resources are available and used online
E.2 Do government departments and local government agencies have websites which are
available in all official languages?
Indicators:
• Government policy to ensure provision of websites with appropriate language access
• Proportion of government departments with websites (value/ranking in UNDESA online services index)
• Quality of government websites (extent of language availability, quantity of content, availability of mobile version)
• Proportion of adult citizens who have used e-government services within twelve months
E.3 Do government and other public stakeholders provide easy online access to

publicly-held data sets, including machine-readable access to original data?
Indicators:
• Legal framework concerning freedom of information
• Number and quantity of open data sets made available by government and available through public access facilities
• Availability of public access facilities that can be used for open data access in e.g. educational institutions and libraries
• Data on the extent of use of open data, in total and within country
E.4 Are provisions concerning the location and duration of data retention consistent with
international standards of data protection and supportive of effective access?
Indicator:
• Legal and regulatory provisions concerning data retention and cross-border data flows
E.5 Can individuals and organisations use and share public data without restriction?
Comment: See above comment about restrictions relating to privacy rights. There ought to be restrictions, therefore this might not be an accurate indicator as presently drafted.
Indicators:
• Legal framework concerning freedom of information
• Presence or absence of restrictions in government policy and practice on the use and sharing of public data
Comment: Care required to clarify that the indicator is not referring restrictions that are consistent with the protection and maintenance of other rights, such as the right to privacy.
E.6 Are open data used by stakeholders in ways which have a positive impact on sustainable development?
Indicators:
• Number of access requests for open data from government
• Evidence of developmental use of open data in selected sectors (e.g. environment, health, agriculture, enterprise)
Children
Comment: The need to ensure that children are properly considered in terms of human rights is supported. The right to privacy and its integral contribution to the development of the personality is particularly relevant here and a relevant consideration for this section of the UNESCO document.
GROUP D – TRUST AND SECURITY
Issues of trust and security are increasingly important to the future of the Internet. As well as the threats to businesses and individuals posed by cybercrime, this theme addresses threats to critical infrastructure and databases which may come from diverse sources, including governments, non-state actors, criminal organisations and individuals.
D.4 Are citizens and businesses taking action to reduce risks to their security and privacy?
Comment: Better as two separate questions or issues such as two questions with wording as below or similar:
· Are citizens taking action to reduce risks to their privacy rights and security online?
· Are business taking action reduce risks to the security of the information they hold, and the privacy obligations they have to individuals?
Indicators:
• Proportions of Internet users with up to date malware protection
• Evidence of business awareness of and contingency plans to counteract cybersecurity attacks
• Extent to which encryption services are used by citizens and businesses
Comment: All of these indicators relate to information security. While related to

privacy, security is not the same thing - privacy rights are much broader.
Only individuals and businesses are mentioned here, is there any intention to analyse government information security practices and practical implementation of privacy rights connected with this issue?
Consideration should be given to and cross-reference made to data/evidence for Category R Question E.5, which is concerned with law and practice concerning encryption and anonymity Are VPNs also relevant here (referred to elsewhere in the document) to protect anonymity? See D6 above.