Submission by ARTICLE 19 to the UN OHCHR in response to the call for inputs to a report on "the right to privacy in the digital age"

Introduction

ARTICLE 19 welcomes the OHCHR's call for inputs to a report on "the right to privacy in the digital age". ARTICLE 19's mission is to defend freedom of expression and information as essential human rights both online and offline. With nine offices globally, we link international advocacy leadership with country-level activities to enhance the reach and effectiveness of both.

Freedom of expression and privacy are mutually reinforcing rights – all the more so in the digital age. Both are essential foundations for open and democratic societies, and among the basic conditions for its progress, and for each individual's self-fulfilment. For democracy, accountability and good governance to thrive, freedom of expression and opinion must be respected and protected. The same is true of the right to privacy, which also acts as a powerful bulwark against state and corporate power in the modern age.[1]

In this submission, we seek to respond to the questions raised by the OHCHR in his call, with a particular focus on questions 4 and 7.

New technologies and standardisation practises enhancing privacy around the world

ARTICLE 19's Digital Programme interfaces with technical standards development organisations (SDOs) on issues relating to human rights, among them privacy and encryption. To date, at least one large and influential SDO, the Internet Engineering Task Force, has adopted privacy guidelines with a view to helping standards developers assess their impact on privacy.[2] This SDO also performs mandatory security impact assessments for all their published standards.

1 ARTICLE 19, The Global Principles on Protection of Freedom of Expression and Privacy, March 9, 2017. https://www.article19.org/resources/the-global-principles-on-protection-of-freedom-of-expression-and-privacy/

2 RFC6973, Privacy Considerations for Internet Protocols. https://tools.ietf.org/html/rfc6973

ARTICLE 19 Free Word Centre 60 Farringdon Road London EC1R 3GA

T +44 20 7324 2500 F +44 20 7490 0566 E expression@article19.org W www.article19.org

Registered in England and Wales 2097222 Registered office: Free Word Centre, 60 Farringdon Road, London EC1R 3GA Registered Charity number 327421

Other similarly influential standards bodies, such as the IEEE 802 LAN/MAN Standards Committee, are drafting privacy guidelines to enhance their future work,[3] while the Internet Corporation for Assigned Names and Numbers (ICANN) recently adopted a new Bylaw that codifies the organisation's commitment to respect internationally recognized human rights as required by applicable law.[4] The application of ICANN's human rights Bylaw in its practical work is still being determined, but we invite the OHCHR to recognise it as a step in the direction of more robust human rights work in international technical governance bodies.

While privacy or human rights guidelines for standards developers are still not part of routine practises in any of the SDOs mapped out by ARTICLE 19, tentative analyses indicate a growing awareness of privacy and security topics among participants in standardisation activities.[5]

Privacy and security are raised at early stages of technology development, rather than added to technologies as an after-thought once the real development is done. Over time, this could increase the robustness of the protection communications infrastructures can afford with respect to privacy, and thereby also reinforce the protection for freedom of expression.

At the same time, companies participating in SDOs may be stuck between the effort of enhancing privacy protections at the lowest technical level, and government demands. An acute example is an individual who self-professed affiliation with law enforcement institutions from the European Union that presented their intention in an SDO of advancing data retention recommendations for Carrier Grade networks at the SDO-level, even after the Court of Justice of the European Union has determined such data retention to be unlawful.[6] While we believe that the technical governance bodies with which ARTICLE 19 engages benefit from giving anyone the opportunity to present ideas at their venues, it is a matter of concern if law enforcement entities make use of these practises in order to circumvent regional laws.

We deem, therefore, that there is a risk in the years ahead that the push for increasing surveillance will shift to international SDOs even after courts have rejected legal mechanisms for obliging such surveillance.

---

3 Public document reposity for the IEEE 802 LMSC Privacy Recommendations Task Group, https://mentor.ieee.org/privecsg/documents

4 By-laws for Internet Corporate of Assigned Names and Numbers, as adopted on May 27, 2016. https://www.icann.org/en/system/files/files/adopted-bylaws-27may16-en.pdf#page=8

5 IETF101 Hackathon presentation by the Datactive BIGBANG research team, London, March 2018. https://github.com/IETF-Hackathon/ietf101-project-presentations/blob/master/MailingListAnalysis-ietf101-presentation.pdf

6 IETF101, Individual draft, Approaches to Address the Availability of Information in Criminal Investigations Involving Large-Scale IP Address Sharing Technologies, Dave O'Reilly (FTR Solutions). https://datatracker.ietf.org/doc/draft-daveor-cgn-logging/

New technologies and standardisation practises that risk harming privacy

While there are reasons to feel optimistic, there are also reasons for concern.

Government-oriented or -steered SDOs, most notably the International Telecommunications Union (ITU), are at risk of reducing the effective scope for privacy and security for individuals by two principal mechanisms: 1) a lack of interest in upholding these human rights, and 2) falling victim to compromises over specific formulations, causing adopted standards to not specify a meaningful level of privacy or security. Such may be the case when a standard introduces many different layers of technical exceptions to privacy or security enhancements, or when a standard presumes increased centralisation of control of a technical system.

Through our presence at the ITU we have been faced with the following problems: a) a lack of transparency in the proceedings of this technical governance body means that neither civil society nor business actors have adequate opportunities to map or follow developments in the body, b) even many governments lack the capacity to fully engage with the multitude of committees that exist within this forum to the extent that they can stake out developments and their own positions with respect to emerging issues.

This is of particular concern as an increasing number of working groups at the ITU seek to address privacy and security topics. While the outcomes of such working groups may indeed gain large impact around the world, contributions to the process of such working groups are limited and may end up reflecting a less rigorous approach to human rights, and in particular to privacy and security of individuals, than should be the case.

We are also wary of initiatives in SDOs that organise, in addition to equipment manufacturers, a few, large customers from especially the telecommunications industry and national standardisations bodies (e.g. 3GPP). Our reservations rest on these observations, which we invite the OHCHR to share:

1) Technical standardisation in the telecommunications sector increasingly aims to place the telecommunications operator as a trust conduit, monopolising implicitly the control over an individuals communications and expression of identity online under the guise of higher security. 2) Security and privacy concerns are proposed to be addressed by shifting responsibility for both to a central point of trust, the telecommunications operator, who is often acting at the mercy of government licensing schemes for electronic communications providers.[7]

7 NGNM White Paper on 5G, in particular sec. 3.2.2:

"On top of supporting the evolution of the current business models, 5G will expand to new ones to

While, as we have argued above, it is desirable that security and privacy are built into the most fundamental levels of technology and while advances in cellular technology standardisation indeed introduce many welcome privacy and security features that will benefit individuals around the world, we believe that proper care should be taken not to make individuals and their rights vulnerable to failures in these central points of trust, or the government policies and licensing schemes upon which these central points of trust depend.

It is the view of ARTICLE 19 that privacy and freedom of expression are ultimately served by avoiding central points of trust (where trust, for all intents and purposes, equates with control) in both technical and legal systems.

ARTICLE 19

ARTICLE 19's mission is to defend freedom of expression and information as essential human rights both online and offline. With nine offices globally, we are able to link international advocacy leadership with country-level activities to enhance the reach and effectiveness of both. In addition to co-chairing the Human Rights Protocol Consideration Research Group at the Internet Engineering Task Force, we founded the Cross Community Working Party at the Internet Corporation for Assigned Names and Numbers (ICANN) on "Corporate and Social Responsibility to Respect Human Rights" and are active in drafting and supporting the passage of privacy guidelines for standards development at the IEEE 802 LMSC, as well as in the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems where we co-chair the working group on "Methodologies to Guide Ethical Research and Design". We maintain steady presence in SG20 and SG17 at the International Telecommunications Union, and co-organise capacity building sessions for civil society organisations that seek to participate in the ITU Plenipotentiary, and we have developed a methodology for performing Human Rights Impact Assessments (HRIAs) in technical infrastructure organisations, such as RIRs and LIRs.

support different types of customers and partnerships. Operators will support vertical industries, and contribute to the mobilization of industries and industry processes. Partnerships will be established on multiple layers ranging from sharing the infrastructure, to exposing specific network capabilities as an end to end service, and integrating partners' services into the 5G system through a rich and software oriented capability set."

https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf