United Nations A/HRC/40/NGO/234

General Assembly

Distr.: General
22 February 2019

English only

Human Rights Council
Fortieth session
25 February–22 March 2019
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written statement* submitted by Human Rights Advocates Inc., a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[12 February 2019]

* Issued as received, in the language(s) of submission only.

GE.19-03081(E)
1903081

The Use of Personal Data by Businesses

I. Introduction

The right to privacy is as important as the sovereign right of nations. It is not only a fundamental freedom under international law, it is also a right declared in over 150 national constitutions.[1] Human rights and fundamental freedoms that people enjoy offline, which are enshrined in the Universal Declaration of Human Rights ("UDHR") and relevant international human rights treaties, including the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights, must equally be guaranteed and protected.[2]

The exercise of human rights in the Digital Age, in particular the right to privacy, is an issue of increasing interest and importance as the rapid pace of technological development allows persons all over the world to use digital technologies. There is no question that the global community needs to undertake urgent action to effectively respect and implement article 12 of the UDHR and article 17 of the ICCPR by developing a comprehensive legal framework on privacy in cyberspace, and to operationalize the respect of this right, domestically and across borders.[3] Unless and until it will be possible for any citizen, anywhere, irrespective of their passport, to enjoy privacy protection without borders and privacy remedies across borders, then it cannot be said that a clear and comprehensive legal framework exists.[4] In order to create such a clear and comprehensive legal framework, it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed, with a commonly agreed set of principles.[5]

II. Background

A. Right To Privacy As It Stands Today

1. Resolutions

While international human rights law provides high level universal rules for the protection of the right to privacy, it lacks the level of detail necessary to provide adequate protection.[6] Most regions in the world lack enforcement mechanisms such as those created over the past 40 years in Europe and North America.[7] Thus the international legal framework would benefit from vastly increased detail, clarity and comprehensiveness, safeguards and remedies for the daily violations of the right to privacy occurring in cyberspace.[8]

During its thirty-seventh session, the Human Rights Council (HRC) adopted a resolution recalling all previous resolutions adopted by the General Assembly (GA) and the HRC on the right to privacy in the digital age.[9]

2. Special Rapporteur

Pursuant to the HRC resolution 28/16, the Special Rapporteur focused its work on surveillance and privacy as they relate to the following thematic action streams: 1) developing a deeper understanding of privacy laws; 2) studying security and surveillance

[1] World constitutions, constituteproject.org, 31 March 2018.
[2] Rapporteur on the Right to Privacy, Prof.Joseph A. Cannataci, 28 February 2018, A/HRC/ 37/ 62.
[3] *Id.*
[4] *Id*.
[5] *Id.*
[6] *Id.*
[7] Report of Special Rapporteur on the Right to Privacy, 28 February 2018, A/HRC/ 37/ 62.
[8] *Id.*
[9] HRC, Privacy In The Digital Age, A/HRC/RES/28/16, 26 March 2015.

issues; 3) defining Big Data and Open Data; 4) researching Health Data; and 5) understanding how businesses use personal data.[10]

The Special Rapporteur has put forth draft text for a Legal Instrument on Government-led Surveillance and Privacy— which will ultimately aid states and the multi-stakeholder community to protect, respect and promote human dignity[11]—as the result of meetings and exchanges between leading global technology companies, experts with experience in working within civil society, law enforcement, intelligence services, academics and other members of the multi-stakeholder community shaping digital technology and the transition to the Digital Age.[12]

Human Rights Advocates (HRA) focuses its research and recommendations on laws governing use of personal data by businesses under the following: the European Union ("EU") General Data Protection Regulation ("GDPR"); the Japan Act on Protection of Personal Information ("APPI"); and the California Consumer Privacy Act ("CaCPA"); these demonstrate how a lack of global uniformity can prove inefficient regardless the sophistication the separate frameworks provide.

III. Analysis

A. The Current Regulatory Framework and Its Impediments, Policy & Practical Implications

1. Problems with the Current Structure

In the age of social media and decentralized networks, technology companies are ubiquitous and their reach is virtually unstoppable. Some of the biggest regulatory challenges to date involve data breaches and data exploitation. Protecting the privacy of individual technology participants is difficult under the current less unified regulatory landscape. Furthermore, and as our research shows, the impediment has less to do with the rigor of a singular framework and more to do with lacking a uniform global definition laying out the standard.

Absent a unified framework, smaller companies lack the resources to adopt every standard required by every jurisdiction. It is often the case that companies resort to cherry picking lax or unregulated jurisdictions while circumventing the more rigorous ones through geo-fencing, a method for virtually excluding specific geographic locations from access to a company's goods or services.[13] This is problematic because the varying standards not only deprive customers of a healthy marketplace, it also stifles growth in smaller companies that lack the resources to comply in all jurisdictions.

2. Territorial Scope of Regulations

The GDPR, as the most rigorous framework, zealously regulates entities' processing of Personal Information ("PI") if such entity: (1) is established in the EU; (2) offers goods or services, irrespective of whether a payment of the individual is required, to individuals in the EU; and (3) monitors behavior of individuals in the EU.[14] Alternatively APPI is a more moderate approach because it applies to any business or organization supplying goods or services to a person in Japan and collecting PI.[15] CaCPA is the narrowest geographic framework as it applies only to organizations doing business in California.[16]

[10] HRC Right to Privacy in the Digital Age, A/HRC/RES/37/2, 22 March 2018,
[11] Report of Special Rapporteur on the Right to Privacy, A/HRC/37/62 (28 February 2018).
[12] *Id.*
[13] Geofencing, International Association of Privacy Professionals, https://iapp.org/resources/article/geofencing/
[14] GDPR, Art 3.
[15] APPI, Art. 75.
[16] CaCPA 1789.

Apart from the concern of extraterritorial reach of GDPR, which many privacy experts view as a potential violation of sovereign rights of nations,[17] the current regulatory structure lacks clear guidance and understanding of basic fundamental issues upon which the regulation is built. It seems somewhat counterintuitive that regulators are zealously enacting Personal Data Privacy laws, but fail to confidently define "personal information"— a core principle.

3. Definitional Gaps - Personal Information

GDPR broadly defines PI as "any information relating to an identified or identifiable natural person."[18] APPI is slightly less ambiguous than GDPR as it defines PI as "any data that is in and of itself personal in nature (e.g., name, date of birth, etc.) and includes unique identifiers assigned to an individual."[19] CaCPA defines PI as "any information that identifies or could identify an individual."[20] Though not exhaustive, CaCPA enumerates some examples of PI, such as purchase history, biometric data, geo-location data.

APPI definition of PI appears to be broader than CaCPA and GDPR by recognizing that there may be types of information that are not actual PI without an identifier.[21] For example, certain types of behavioral information (e.g., cookies, etc.) could be considered non-PI under the APPI if the identifiers are removed, while the CaCPA and GDPR may require a further analysis of whether the behavioral information identifies an individual.[22]

IV. Recommendations

Recently, AT&T, Google, Amazon, Twitter and Apple testified in United States of America Senate hearings in favor of a unified privacy and data security law covering consumer personal data.[23] Each offered its own frameworks -- a simplified version of GDPR -- but there is agreement on some ideas: calling for a standard definition of PI, letting consumers access and correct their personal data (deleting information as needed) and setting basic data security standards.[24]

While HRA agrees in part with the regulatory changes discussed in the Senate hearing, we also urge the Special Rapporteur to consider the following recommendations for the use of personal data by businesses:

- To adopt a single overarching definition for PI, which shall include an exhaustive list of qualifiers and exclusions;
- To adopt, or use as template, the most rigorous standard (such as GDPR) that overlaps with other frameworks and to which companies are already compliant;
- To encourage "whitelisting" where jurisdictions with similar standards recognize each other's frameworks as valid;
- To add carve-out provisions to the final resolution allowing financial institutions as well as healthcare companies, which already comply with similar regulations such as HIPPA and GLBA, to avoid the inefficiency of double-reporting.

---

[17] GDPR: Europe's Tariffs by Other Means, Daniel Lyons, http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/,03, July, 2018.
[18] GDPR, Art. 4(1)
[19] APPI, Art. 2(1), (3), (6)-(7)
[20] CaCPA 1789.140(o)
[21] APPI to Align WIth GDPR, Michihiro Nishi, Skadden Arps, 24, September, 2018.
[22] APPI, Art. 2.
[23] Yeki Faitelson, Data Privacy Disruption In The U.S., Forbes.com (link),12 December 2018.
[24] *Id.*