Submission to the Report of Privacy in the Digital Age

The right to privacy is a fundamental freedom under articles 12 of the Universal Declaration of Human Rights ("UDHR") and 17 of the International Covenant on Civil and Political Rights ("ICCPR"). Both provisions state: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his [honor] or reputation. Everyone has the right to the protection of the law against such interference or attacks." Today's technological advancements bring new meaning to the right to privacy.

In its twenty-eighth session, the Human Rights Council ("HRC") reaffirmed the human right to privacy, "according to which no one shall be subject to arbitrary or unlawful interference," and the right to "the protection of the law against such interference."[1] The HRC has emphasized that States must comport with human rights obligations regarding the right to privacy when they "intercept digital communications . . . and/or collect personal data and when they require disclosure of personal data from third parties, including private companies."[2]

The Special Rapporteur on the Right to Privacy recommends formulating a detailed and universal understanding of the "right to privacy" by developing a clear and binding definition of the right.[3] The Office of the United Nations High Commissioner for Human Rights ("OHCHR") has prepared a report on the right to privacy in the digital age, identifying issues regarding the underlying meanings of the language found in article 12 of the UDHR and article 17 of the ICCPR with respect to "interference with privacy," "arbitrary nor unlawful," and "protection of law."[4] Below, HRA examines these terms with examples of how to make regulations compliant with human rights obligations, then observes how the Human Rights Committee is holding member States accountable under the ICCPR. Last, HRA respectfully recommends the HRC affirm that mass surveillance and data retention programs interfere with the right to privacy; develop language on consent, transparency, judicial oversight, and adequate remedies for violations; and affirm actions furthering Human Rights Committee recommendations on surveillance and data retention.

I. Mass Surveillance, Metadata Retention, and Privacy

The slightest possibility that communications may be surveilled or captured interferes with privacy because of potential chilling effects it can have on free expression or free association.[5] Retention of metadata interferes with privacy because of its potential to be just as revealing as the content of communications (such as a user's age, religion, address, occupation, passwords, etc.).[6] Mass surveillance and retention of metadata both have the potential to result in large scale human rights abuses.

A. Interference with Privacy

The European Court of Justice, in response to the EU Data Retention Directive allowing States to rely on third parties to retain and provide metadata of individuals,[7] explains that whether the right to privacy is interfered upon by governments or

[1] Human Rights Council Res. 28/16, preamble, U.N. Doc. A/HRC/RES/28/16 (Apr. 1, 2015).
[2] *Id.* at 2-3.
[3] Report of the Special Rapporteur on the Right to Privacy, ¶ 20-21, U.N. Doc. A/HRC/31/64 (advanced unedited version) (Mar. 8, 2016).
[4] Report of the Office of the United Nations High Commissioner for Human Rights, ¶ 12, U.N. Doc. A/HRC/27/37 (June 30, 2014) (hereinafter "OHCHR").
[5] *Id.* ¶ 20.
[6] Access Now, *Review of the e-Privacy Directive*, 7 (Dec. 2016), https://www.accessnow.org/cms/assets/uploads/2016/12/Access-Now-ePrivacy-Directive-policy-paper.pdf.
[7] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 1 (Apr. 18, 2011), https://www.eff.org/files/filenode/dataretention/20110418_data_retention_evaluation_en_0.pdf.

third parties is immaterial: it is an interference upon the right to privacy to retain metadata, period.[8] Per the OHCHR, the "very existence of a mass surveillance [program] [] creates an interference with privacy."[9] For example, South Africa's Regulation of Interception of Communications and Provision of Communication-Related Information Act requires telecommunications providers to store metadata for up to five years.[10] This regulation is a per se interference with privacy and requires safeguards to ensure it is neither arbitrary nor unlawful.

B. Neither Arbitrary nor Unlawful

To ensure interference is neither arbitrary nor unlawful, State regulations should require third parties to obtain explicit consent from users of technology services where retention of data and metadata and its accessibility to the state is possible A provision giving users control through consent will ensure the law is not arbitrary provided it is "sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances."[11] For example, India's Information Technology Rules under the Information Technology Act requires cyber cafes to retain user identification, information, and browsing history for one year and must provide the data if requested by authorized authorities.[12] To comply with international law, India's IT Act must require explicit user consent before cyber cafes, and other similar entities, can retain user information and data.

C. Protection of Law

To give the "protection of the law" against interference with the right to privacy, States must institute procedural safeguards to ensure any wrongdoing by the State is accordingly dealt with and actions are put in place to prevent future wrongdoing. Such safeguards include creating independent and impartial judicial oversight mechanisms to review cases of misconduct; making available adequate remedies to those who are harmed by unlawful government surveillance or metadata retention; as well as transparency measures, as most individuals never become aware of the infringement of their privacy by States.[13] Identifying adequate remedies involves making available remedies "known and accessible to anyone with an arguable claim" of violation, along with a "prompt, thorough and impartial" investigation, with the ability to end ongoing violations, and mandating criminal prosecution for gross violations of privacy.[14]

Thailand's Telecommunications Business Act B.E. 2544 ("TBA") grants the government broad power to maintain public order, national security, economic stability, or to protect public interests, which includes taking possession of devices and equipment used by licensed telecommunications providers, their services, as well as order their employees to take certain actions until the end of the necessity.[15] Thailand's TBA regulation includes no judicial oversight and lends itself to potential abuse.

II. Human Rights Committee

In monitoring the ICCPR, The Human Rights Committee is holding States accountable to their obligations related to the right to privacy with respect to digital privacy. For instance, South Korea's Telecommunications Business Act allows government actors to obtain subscriber information from telecommunications operators for investigatory purposes without a warrant, and insufficiently regulates wiretapping by the National Intelligence Service.[16] Similarly, Macedonia security services have allegedly committed extensive wiretapping of opposition politicians and journalists without notification or access to adequate remedies.[17] Great Britain's Data Retention and Investigatory Powers Act of 2014 allows for broad powers

---

[8] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Comm'ns, 2014 C.J.E.U., ¶ 34.
[9] OHCHR, supra note 4, ¶ 20.
[10] Privacy International, Stakeholder Report to the Universal Periodic Review 27th Session—South Africa, *The Right to Privacy in South Africa*, ¶ 20 (Oct. 2016), https://www.privacyinternational.org/node/999.
[11] OHCHR, supra note 4, ¶ 23.
[12] Privacy International, Stakeholder Report to the Universal Periodic Review 27th Session—India, *The Right to Privacy in India*, ¶ 40 (Oct. 2016), https://www.privacyinternational.org/node/995.
[13] OHCHR, supra note 4, ¶ 38.
[14] *Id.* ¶ 40.
[15] Privacy International, *Who's That Knocking at My Door? Understanding Surveillance in Thailand*, 17 (Jan. 2017), https://www.privacyinternational.org/node/1345.
[16] Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the Republic of Korea, ¶ 42, U.N. Doc. CCPR/C/KOR/CO/4 (Dec. 3, 2015).
[17] Human Rights Committee, Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, 5, U.N. Doc. CCPR/C/MKD/CO/3 (Aug. 17, 2015).

of communications data retention where access is not limited to the most serious crimes.[18] In all of these situations, the Committee has explicitly called upon each State to review its regulations and ensure compliance with the ICCPR and the right to privacy.[19]

III. Recommendations

The HRC has noted that public security concerns may justify interference with privacy, but States must ensure that any measures taken in this regard comply with their obligations under human rights law.[20] To that end, HRA respectfully puts forth the following recommendations to the HRC for inclusion in its resolutions on the right to privacy:

- Affirm that mass surveillance programs and metadata retention, by either government or private parties, is an infringement upon the right to privacy.
- Request States to obtain explicit and positive consent from individuals in order to retain metadata and to be clear as to the use of such information.
- Request States to introduce systems of transparency and judicial oversight, and provide for adequate remedies, for those whose right to privacy is wrongfully violated.
- Affirm the Human Rights Committee's actions furthering its recommendations to member States to uphold the right to privacy and not to infringe on individuals' fundamental rights and freedoms when implementing communications surveillance laws or data retention policies.

[18] Human Rights Committee, Concluding Observations on the Seventh Periodic Report of the Kingdom of Great Britain and Northern Ireland, 7, U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17, 2015).
[19] *See* U.N. Docs CCPR/C/KOR/CO/4, CCPR/C/MKD/CO/3, and CCPR/C/GBR/CO/7.
[20] Human Rights Council Res. 28/16, supra note 1, preamble.