P.O. Box 5675, Berkeley, CA 94705 USA

The Right to Privacy: Mass Surveillance and Metadata Retention by States

Contact Information:
Nicole Beckley, Frank C. Newman Intern
mnbeckley@usfca.edu
Representing Human Rights Advocates through
University of San Francisco School of Law's
International Human Rights Clinic
Tel: 415-422-6961
Professor Connie de la Vega
delavega@usfca.edu

I. Introduction

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.

At 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," as well as the right to "the protection of the law against such interference."[1] The HRC has emphasized that States must comport with human rights obligations with regard to 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 HRC also recognizes the need to discuss issues relating to the right to privacy in the digital age, including: "procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices."[3]

In this same session, the HRC issued a mandate to the Special Rapporteur on the Right to Privacy with the task of gathering information related to national practices, study trends,

---

[1] Human Rights Council Res. 28/16, The right to privacy in the digital age, pg. 2, U.N. Doc. A/HRC/RES/28/16 (Apr. 1, 2015).
[2] *Id.* at 2-3.
[3] *Id.*

developments, and challenges related to the right to privacy and to report back to the HRC with proposals and recommendations to promote the right to privacy.[4] The Special Rapporteur recommends developing a more detailed and universal understanding of what is meant by "right to privacy" by developing a clearer definition of the right.[5] To assist in this matter, this paper will use examples of State legislation and actions that violate the right to privacy and illustrate how these scenarios can help define the right to privacy as it relates to digital privacy.

The Office of the United Nations High Commission for Human Rights 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."[6] These three issues will form the basis of Human Rights Advocates' ("HRA") recommendations on how to address defining the right to privacy in a clear, meaningful manner that will give States a firm understanding on how to comply with their obligations to the right to privacy under the ICCPR and UDHR. HRA will also address how the dynamic between States and corporations can impact human rights and will provide examples on how corporate compliance with international human rights standards will help States to also comply with those standards. Lastly, HRA will provide current examples on how the Human Rights Committee under the ICCPR is already taking positive action toward holding State Parties accountable to their right to privacy obligations under the ICCPR.

---

[4] *Id.* at ¶ 4.
[5] 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) [hereinafter *Special Rapporteur*].
[6] 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"].

II. Mass Surveillance and Metadata Retention

Mass surveillance can be defined as "[a]ny system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals."[7] Due to technological advancements, mass surveillance can be accomplished with greater ease and at larger magnitudes than ever before, creating serious concerns about arbitrary and disproportionate interference with the right to privacy. Governments can spy on individuals using any number of technologies, including through the use of closed-circuit television cameras, cell phone towers, and by requiring telecommunication companies to store and make available customer data or metadata.[8]

In 2014, former Australian Prime Minister Tony Abbott infamously referred to metadata as the "envelope" and not the "letter," implying metadata to be innocuous, revealing nothing more than a stamp or address on an envelope would reveal.[9] That statement largely undercuts the significance of metadata and the amount of personal information it can reveal, including a user's age, religion, address, occupation, passwords, and so on.[10] Although metadata is not the same as content data, metadata is the "data about data" and can consistent of the location a sent communication originated from, the type of device that sent the communication, the time the message was sent, and the recipient of the communication and their location, device, and

---

[7] Privacy International, *Mass Surveillance*, https://www.privacyinternational.org/node/52 (last visited Feb. 20, 2017).
[8] *Id.*
[9] Josephine Tovey, *Metadata policy done on the back of an* envelope, THE SYDNEY MORNING HERALD, Aug. 9, 2014, http://www.smh.com.au/comment/metadata-policy-done-on-the-back-of-an-envelope-20140806-10149p.html.
[10] Access Now, *Review of the e-Privacy Directive*, pg. 7 (Dec. 2016), https://www.accessnow.org/cms/assets/uploads/2016/12/Access-Now-ePrivacy-Directive-policy-paper.pdf.

time received.[11] The retention of metadata creates an interference with privacy because metadata can reveal so much about a user. There is some evidence that metadata retention has very little effect on deterring crime, such as a study done in Germany finding "indiscriminate and blanket telecommunications data retention had no statistically relevant effect on crime or crime clearance trends."[12] This evidence supports the conclusion that metadata retention alone is unnecessary and disproportionate.

It is an interference with privacy when communications are surveilled or captured because of the chilling effects it can have on free expression or free association.[13] Mass surveillance and retention of metadata both have the potential to result in large scale human rights abuses and ought to be curtailed by holding States accountable to their right to privacy obligations. A way to encourage this accountability is to ensure a clear definition of right to privacy is formulated—a definition that clearly and concisely sets the standards by which States are to protect the right to privacy of all individuals within their borders and beyond is needed.

III. Interference with Privacy

Articles 12 and 17 of the UDHR and ICCPR both provide that no one shall be subjected to an interference of their privacy. The European Court of Justice, in response to the EU Data Retention Directive in which a State could rely on third parties to retain and provide metadata

[11] Privacy International, *Metadata*, https://www.privacyinternational.org/node/53 (last visited Feb. 22, 2017).
[12] German police statistics prove telecommunications data retention superfluous, Stoppt die Vorratsdatenspeicherung!, June 6, 2011, http://www.vorratsdatenspeicherung.de/content/view/455/79/lang,en/
[13] OHCHR, *supra* note 6, at ¶ 20.

of individuals,[14] has stated that whether the right to privacy is interfered upon by governments or third parties is immaterial: it is an infringement upon the right to privacy to retain metadata, period.[15] Likewise, the "very existence of a mass surveillance [program] [] creates an interference with privacy."[16] Although direct, the provision is silent as to what an "interference" actually entails.

South Africa's constitution acknowledges a right to privacy in section 14 where: "[e]veryone has the right to privacy, which includes the right not to have:

(a) Their person or home searched;
(b) Their property searched;
(c) Their possessions seized;
(d) The privacy of their communications infringed."[17]

This definition from the South African constitution can be used as an example of how to more clearly define what an interference with privacy entails, such as not having personal property searched or private communications infringed upon. Unfortunately, this definition also leaves the term "infringed" vague and unclear. Perhaps due to this lack of clarity, South Africa has also implemented the Regulation of Interception of Communications and Provision of Communication-Related Information Act ("RICA") which requires telecommunications providers

[14] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), pg. 1 (Apr. 18, 2011), https://www.eff.org/files/filenode/dataretention/20110418_data_retention_evaluation_en_0.pdf.
[15] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Comm'ns, 2014 C.J.E.U., ¶ 34.
[16] OHCHR, *supra* note 6, at ¶ 20.
[17] S. AFR. CONST., Seventeenth Amendment Act of 2012, Ch. 2 § 14.

to store metadata for up to five years.[18] South Africa's RICA regulation would be considered an interference with privacy according to the European Court of Justice merely for existing. To bring the South African constitution more in compliance with the right to privacy, their constitution ought to also include a provision holding that a person shall not have their possessions or metadata seized. To help States like South Africa to ensure compliance with the right to privacy, HRA recommends the HRC, like the European Court of Justice, resolve that the retention of metadata is a per se interference with privacy. This will help clarify the definition of right to privacy, which will give States notice that all mass surveillance and data retention programs are per se infringements and there must be safeguards in place.

IV. Neither Arbitrary nor Unlawful

Under the ICCPR, an interference cannot be arbitrary and the High Commissioner further states that the interference cannot be unlawful as well.[19] An arbitrary interference would go directly against the necessity and proportionality principles introduced by the HRC.[20]

To ensure interference is neither arbitrary nor unlawful, States should provide in their data regulation regimes that third parties must obtain the explicit consent from users of the technology services where the retention of data and metadata and its accessibility to the State is a possibility. A consent provision gives users control and will ensure the law is neither arbitrary nor unlawful so long as 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

[18] 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.
[19] OHCHR, *supra* note 6, at ¶ 15.
[20] Human Rights Council Res. 28/16, *supra* note 1.

under what circumstances."[21] Even an Advisory Committee to the U.S. Department of Health in 1973 recognized that "[t]here must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent."[22]

One example of legislation that has the potential to be arbitrary and unlawful is found in India's constitution, which allows restrictions on the right to privacy "in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to offense."[23] These restrictions would give broad powers to the government to justify an infringement upon privacy. One such example where a regulation could be considered arbitrary and unlawful is India's Information Technology Rules under the Information Technology Act ("IT Act") which requires cyber cafes to retain user identification, information, and browsing history for one year and must provide the data if requested by authorized authorities.[24] Generally, the IT Act also permits any "authorized public official to intercept communications on the occurrence of any public emergency or in the interest of public safety."[25] Due to the broad powers granted under the IT Act, India can impose wide-reaching nets for private communications and metadata. These nets are arbitrary in that much of the information obtained would be irrelevant to any emergency or issue of public safety, and thus

[21] OHCHR, *supra* note 6, at ¶ 23.
[22] DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, pg 41, U S Govt. Printing Office, Washington USA (1973).
[23] Privacy International, Stakeholder Report to the Universal Periodic Review 27th Session—India, *The Right to Privacy in India*, ¶ 10 (Oct. 2016), https://www.privacyinternational.org/node/995.
[24] *Id.* at ¶ 40.
[25] *Id.* at ¶ 14.

would be unnecessary and disproportionate to the issue requiring the information, and therefore arbitrary. It would also be unlawful because it would not give telecommunication service users or cyber café customers, for instance, the ability to deny the use of their private information. Were India to introduce law requiring third parties, like telecommunications companies or cyber cafes, to require positive and explicit consent from users in order to store data with the understanding that it may be provided to the government in specific circumstances, then India would be closer to being in compliance with its obligations with respect to right to privacy.

To counter the effects of arbitrary or unlawful regulation, HRA recommends that the HRC urge States to require explicit and informed consent of users if the government or third parties are to retain user metadata or intercept private communications.

V. 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 would include creating independent and impartial judicial oversight mechanisms to review cases of misconduct and to make available adequate remedies to those who are harmed by unlawful government surveillance or metadata retention.[26] Included in these safeguards is the necessity of transparency, as most individuals never become aware of the infringement of their privacy by States.[27] Identifying adequate remedies involves making available remedies "known and accessible to anyone with an arguable claim" of violation, along with a "prompt, thorough and

[26] *Id.* at ¶ 38.
[27] *Id.*

impartial" investigation, with the ability to end ongoing violations, and mandating criminal prosecution for gross violations of privacy.[28]

An example of legislation that lacks these necessary safeguards is Thailand's Telecommunications Business Act B.E. 2544 ("TBA"), which 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.[29] Thailand also created the National Council for Peace and Order ("NCPO") and bestowed upon this group broad powers to "[prevent] and [suppress] offenses relating to lèse-majesté, internal security, firearm regulations, and 'any violation of any other orders issued by the NCPO.'"[30] The NCPO flexed such power by establishing a committee tasked with accessing and examining social media information with the ability to "suspend or close websites and social media platforms . . . accused of undermining the military government."[31] Neither the TBA nor the NCPO are subject to judicial oversight.[32] Due to the large potential for abuse, the TBA and NCPO must be tempered by judicial oversight to ensure that any wrongdoing is immediately stopped and future wrongdoing is prevented. They must also incorporate elements of transparency in order for users to know if their information has

[28] *Id.* at ¶ 40.
[29] Privacy International, *Who's That Knocking at My Door? Understanding Surveillance in Thailand*, pg. 17 (Jan. 2017), https://www.privacyinternational.org/node/1345.
[30] *Id.* at 16 (citing Telenor Group, *Authority Requests for Access to Electronic Communication—legal overview*, May 2015, https://www.telenor.com/wp-content/uploads/2015/05/GOVERNMENT-ACCESS-REPORT_05.pdf.).
[31] *Id.* at 17.
[32] *Id.*

been improperly stored or intercepted by the government, and proper remedies must be in place to provide redress to those whose rights were infringed upon.

HRA would request the HRC resolve that judicial oversight, adequate remedies, and transparency safeguards are necessary to ensure surveillance and data retention programs are in compliance with the right to privacy under the ICCPR.

VI. Responsibilities of Corporations and Third Parties

The Special Representative of the Secretary General on the issue of human rights and transnational corporations has identified three pillars as part of the "Protect, Respect and Remedy" framework developed to address human rights violations: First, States have a duty to protect against violations of human rights by third parties; second, corporations have the responsibility to respect human rights, including using due diligence to avoid human rights infringement and to address head-on any adverse involvement.[33] In response to this Framework, a number of recommendations to State Parties were developed and presented as Guiding Principles.[34] Although human rights obligations currently only apply to State governments, the Guiding Principles presented by the Special Representative will "[elaborate] [on] the implications of existing standards" and integrate them into regular business practices in order to advance human rights protections.[35] The following suggestions are given in the same vein, knowing that corporations are not obligated by treaty to respect human rights principles, but also recognizing that States can hold corporations accountable by creating regulatory schemes that require certain compliance with human rights norms by third parties.

---

[33] *Special Rapporteur*, *supra* note 5, at ¶ 6.
[34] Id. at ¶ 13.
[35] Id. at ¶ 14.

In many of the examples presented above, State governments have required third party companies to retain metadata and to provide such information upon request. These companies have a responsibility to ensure that, when "faced with government demands for access to data that do not comply with international human rights standards" the company must do everything in their power to respect human rights principles in a demonstrable way, such as narrowly interpreting government demands, obtaining clarification regarding the scope and legal foundation for the demand, requiring a court order, and being transparent with users regarding compliance with the government's demand.[36]

VII. Human Rights Committee

The Human Rights Committee has been consistently reminding States of their obligations to protect privacy under the ICCPR. For example, South Korea's Telecommunications Business Act allows government actors to obtain subscriber information from telecommunications operators for investigatory purposes without a warrant, as well as insufficiently regulates wiretapping by the National Intelligence Service.[37] The Human Rights Committee recommended that South Korea make the necessary legal amendments needed to ensure surveillance is compatible with the ICCPR and the right to privacy by requiring subscriber information not to be provided to the government without a warrant and to introduce monitoring mechanisms for communication investigations by the National Intelligence Service.[38]

[36] OHCHR, *supra* note 6, at ¶ 45.
[37] 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).
[38] *Id.* at ¶ 43.

Similarly, Macedonia security services have allegedly committed extensive wiretapping of opposition politicians and journalists without notification or access to adequate remedies.[39] The Human Rights Committee has requested the State ensure its surveillance activities conform to the obligations under the ICCPR, specifically that all interference with the right to privacy measures comport with the legality, proportionality and necessity principles and that persons unlawfully monitored are notified of such monitoring and given access to adequate remedies.[40]

Another example is Great Britain's Data Retention and Investigatory Powers Act of 2014 allows for broad powers of communications data retention where access is not limited to the most serious crimes.[41] The Human Rights Committee addressed these concerns and issued recommendations that the UK must ensure that any interference with the right to privacy under the current legal regime complies with: "the principles of legality, proportionality and necessity"; is authorized by law, tailored to specific legitimate aims, and provides for effective safeguards against abuse; that judicial oversight is in place in order to prevent abuses; that interference is limited to only the most serious crimes; and that there are effective remedies available to victims of abuse.[42]

In these examples, the Human Rights Committee has explicitly called upon each State to review their regulations and ensure they are in compliance with the ICCPR and the right to

[39] Human Rights Committee, Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, pg. 5, U.N. Doc. CCPR/C/MKD/CO/3 (Aug. 17, 2015).
[40] *Id.*
[41] Human Rights Committee, Concluding Observations on the Seventh Periodic Report of the Kingdom of Great Britain and Northern Ireland, pg. 7, U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17, 2015).
[42] *Id.*

privacy.[43] This illustrates how the Human Rights Committee is taking positive actions toward holding States accountable under the right to privacy with respect to digital privacy and serves to encourage the HRC to likewise urge State Parties to comply with their right to privacy obligations under the ICCPR and UDHR.

By holding States accountable to their privacy obligations by defining an interference with privacy to include mass surveillance and metadata retention, that any such interference programs are neither arbitrary nor unlawful by requiring user consent, and through the implementation of safeguards such as judicial oversight, adequate and available remedies, and transparency, the right to privacy will be more clearly understood and States will understand how to ensure they are in compliance with their privacy obligations.

VIII. Conclusion

The difficulty with holding State Parties accountable to their obligations under the ICCPR with respect to the right to privacy lies in the vague understanding of what the "right to privacy" actually entails. This paper supports the notion that to give understanding to what the right to privacy includes, there must be firm definitions of the terms "interference with privacy," "neither arbitrary nor unlawful," and "protection of law." Through the aforementioned examples, ways to define these terms include recognizing mass surveillance and metadata retention as per se interference with the right to privacy, that nonspecific and wide scale surveillance and metadata retention without user consent is arbitrary and unlawful, and that protection of law requires judicial oversight mechanisms and access to remedies. It is

[43] *See* Republic of Korea, U.N. Doc. CCPR/C/KOR/CO/4, *supra* note 37; Third Periodic Report of the Former Yugoslav Republic of Macedonia, U.N. Doc. CCPR/C/MKD/CO/3, *supra* note 39; and Kingdom of Great Britain and Northern Ireland, U.N. Doc. CCPR/C/GBR/CO/7, *supra* note 41.

also important to recognize the role of corporations in respecting human rights due to the way corporations are often the tool by which governments infringe upon individuals' rights to privacy. Finally, it is important to acknowledge the positive steps taken by the treaty bodies in beginning to hold State Parties accountable where certain regulations or legislations appear to fall short of their human rights obligations. By elucidating a clearer definition of what it means to have a right to privacy, the more specific and effective treaty body recommendations and HRC resolutions will be when it comes to respecting and protecting the right to privacy.

IX. Recommendations

Human Rights Advocates respectfully puts forth the following recommendations and urges the Human Rights Council:

1. To affirm that mass surveillance programs and the retention of data, by either government or private parties, is an infringement upon the right to privacy.
2. To request States to obtain explicit and positive consent from individuals in order to retain metadata and be clear as to what use such information is for.
3. To request States to introduce systems of transparency and judicial oversight, as well as provide for adequate remedies, for those whose right to privacy is wrongfully violated.
4. To support the actions taken by the Human Rights Committee where recommendations have been made to member States to uphold the right to privacy and to not infringe on individuals' fundamental rights and freedoms when implementing communications surveillance laws or data retention policies.