How to Apply the ICCPR Privacy Exceptions Regime to State-Sponsored Mass Surveillance

Laura Zecca, GW Law '25

September 2025

I. Introduction

On November 7, 2024, the United Nations Human Rights Committee ("HRC" or "the Committee") published its concluding observations on Pakistan's compliance with the International Convention on Civil and Political Rights ("ICCPR").[1] The Committee expressed concern over the Pakistani government's unchecked authority to conduct mass surveillance of its citizens and targeted surveillance of "human rights defenders, journalists, political activists, politicians and individuals critical of the Government."[2] By ratifying the ICCPR, Pakistan undertook the obligation to protect the right to privacy, among others. And although a State party may infringe upon the right to privacy under certain circumstances,[3] it may only do so within delineated bounds.[4] Out of its concern, the Committee recommended that Pakistan take measures to ensure its surveillance laws align with its ICCPR obligations.[5]

The HRC requires surveillance legislation and the state's application to comply with "the principles of legality, proportionality and necessity."[6] Although the HRC recommended that Pakistan adopt a legislative framework for surveillance that aligns with these principles, the Committee did not advise Pakistan—nor has it advised any state—on precisely what compliance entails.[7] This Article examines HRC jurisprudence to determine the extent to which ICCPR parties can conduct mass surveillance while remaining in alignment with these key principles and, in turn, their obligations under the ICCPR. In sum, indiscriminate mass surveillance by a state will never satisfy the principles of legality, proportionality and necessity.

The Pakistani government conducts mass surveillance of its own citizens in the name of protecting national security virtually unrestricted because its legislative framework grants broad surveillance powers to the federal government without providing for judicial or regulatory

---

[1] Human Rights Committee, Concluding observations on the second periodic report of Pakistan, CCPR/C/PAK/CO/2 (Nov. 7, 2024) [hereinafter HRC Concluding Observations].
[2] *Id.* at 44.
[3] International Covenant on Civil and Political Rights, Art. 17, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR] (available here); Arturo J. Carrillo, *The Price of Prevention: Anti-Terrorism Pre-Crime Measures and International Human Rights Law*, 60 VA. J. INT'L L. 571, 647 (2020) (available here).
[4] ICCPR, *supra* note 3, arts. 12(3), 9, 14(1), 19(3)(b), 21, 22(2); Carrillo, *supra* note 3, at 648 (citing Human Rights Committee, General Comment No. 27, ¶¶ 14, 18, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. 1) (Nov. 2, 1999); U.N. COUNTER-TERRORISM IMPLEMENTATION TASK FORCE, BASIC HUMAN RIGHTS REFERENCE GUIDE: CONFORMITY OF NATIONAL COUNTER-TERRORISM LEGISLATION WITH INTERNATIONAL HUMAN RIGHTS LAW, at 11, diagram 1.5 (Oct. 2014), https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/counterterrorismlegislation.pdf.
[5] HRC Concluding Observations, *supra* note 1, at 45.
[6] *Id.*
[7] *Id.*

oversight.[8] The Pakistani government has even defied judicial attempts to check its use of mass surveillance. In July 2024, the Federal Government, through the Ministry of Information Technology and Telecommunication ("MoITT"), authorized the Inter-Services Intelligence Agency (ISI) to intercept and trace calls, and monitor individuals' digital communication.[9] The MoITT did so seemingly in opposition to an order of the Islamabad High Court, which "explicitly prohibit[ed]" such surveillance and questioned the legality and lack of authorization for such surveillance.[10] In October 2024, the judiciary's limited ability to check the political branches was effectively dismantled with the passage of Pakistan's newest constitutional amendments.[11] The amendments enhanced the political branches' involvement in the judiciary by permitting a reconstituted judicial commission consisting of more ruling coalition appointees as members to hand select judge panels that will hear *any* constitutional case in Pakistan.[12] Cases involving surveillance, which implicates a Pakistani constitutional question, will therefore be heard by a cherry-picked group of judges.[13]

Pakistan has taken increasingly extreme measures to maintain and grow its online surveillance systems by purchasing powerful foreign technology. In 2018, the government entered into a five-year contract with Canadian company Sandvine for its web management system, which allows the government to manage internet traffic and conduct Deep Packet Inspection ("DPI").[14] DPI is a highly invasive tool that can intercept, analyze, and decrypt data—its function works akin to an airport scanner, permitting the "authorities to look inside the data packets travelling across the internet and check their contents for sensitive information."[15] As of 2024, the government has purportedly purchased Chinese technology to implement an even stronger internet "firewall" that will enable Pakistani authorities to monitor internet traffic, which results in reduced internet speed and access.[16] While the government has built up its firewall, it has also cracked down on the use of VPNs, which citizens have relied on to navigate the internet without being subjected to the firewall's tracking and blockages.[17]

Pakistan has created and further strengthened its surveillance state despite its constitutional guarantee of the right to privacy and its international obligations under the ICCPR. It is in this context that the ICCPR's right to privacy is under siege; the question is how can Pakistan better

---

[8] *Id.* at ¶¶ 44, 45; *see also Pakistan: Submission to the UN Human Rights Committee 142nd session, 14 October – 8 November 2024*, Amnesty International, ASA 33/8576/2024 13–14 (Sept. 23, 2024) (available here).
[9] HRC Concluding Observations, *supra* note 1, at 44; Mariyam Suleman Anees, *Pakistan Expands Surveillance Powers Yet Again in the Name of 'National Security',* The Diplomat (July 31, 2024), https://thediplomat.com/2024/07/pakistan-expands-surveillance-powers-yet-again-in-the-name-of-national-security/.
[10] Anees, *supra* note 9; Umer Mehtab, *IHC says those involved in and aiding surveillance of citizens are 'liable for offences,'* Dawn (May 30, 2024), https://www.dawn.com/news/1836404.
[11] *Pakistan: 26th Constitutional amendment is a blow to the independence of the judiciary*, International Commission of Jurists (Oct. 21, 2024), https://www.icj.org/pakistan-26th-constitutional-amendment-is-a-blow-to-the-independence-of-the-judiciary/.
[12] *Id.*
[13] *Id.*; Sahar Iqbal, *The legal landscape for privacy and surveillance in Pakistan*, International Bar Association (June 20, 2023), https://www.ibanet.org/legal-landscape-for-privacy-surveillance-in-Pakistan.
[14] Abid Hussain, *Pakistan tests secret China-like 'firewall' to tighten online surveillance*, Al Jazeera (Nov. 26, 2024), https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance.
[15] *Id.*
[16] Hussain, *supra* note 14.
[17] *Id*.

protect that right and others while fulfilling its duty to protect public safety and national security? This Article seeks to respond to that question. It proceeds in two parts. Part II explains the basis of the right to privacy in international law and the challenges of protecting that right in light of the rapid development of technology. Part III discusses the legal framework of the right to privacy's "Exceptions Regime" and analyzes how UN bodies, particularly the HRC, have applied the Exceptions Regime to extrapolate the requirements for conducting state-sponsored surveillance without violating ICCPR obligations. The Article concludes by providing parties to the ICCPR, including Pakistan, a framework for compliance with the Exceptions Regime when conducting surveillance for the sake of protecting national security.

II. The Right to Privacy in International Law

Article 17 of the ICCPR provides that no individual "shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence" and declares that "[e]veryone has the right to the protection of the law against such interference or attacks."[18] When the parties drafted the ICCPR in 1966, none could have anticipated the attack the right to privacy would face in the digital age.[19] As the world has experienced rapid technological advancements, the Committee and other UN bodies have taken action to ensure the right to privacy is not subjected to an originalist interpretation.

A. Expansion of Right to Privacy in the Digital Age (1988-2013)

The HRC took its first major step in guaranteeing the right to privacy in 1988 with the adoption of General Comment No. 16 ("GC 16").[20] GC 16 clarified that both government authorities and individuals are obligated to respect each individual's right to privacy and that all ICCPR parties are required to adopt legislative measures "to give effect to the prohibition against such interference and attacks" in order to protect the right.[21] The Committee specifically addressed technological developments, requiring that "[t]he gathering and holding of personal information on computers, databanks and other devices . . . be regulated by law."[22]

Several UN Special Rapporteurs[23] turned their attention to states' increased level of surveillance in the post-9/11 world, as many justified broad surveillance practices for the purpose of combating terrorism.[24] The UN Special Rapporteur on the Promotion and Protection of Human

[18] ICCPR, *supra* note 3, art. 17.
[19] ICCPR, *supra* note 3.
[20] U.N. Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1, at 21 (Apr. 8, 1988), https://documents.un.org/doc/undoc/gen/g94/189/63/pdf/g9418963.pdf [hereinafter GC 16]; Asaf Lubin, *A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens*, Digital Repository at Maurer Law, at 14, n. 62 (Sept. 21, 2017), https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3911&context=facpub.
[21] GC 16, *supra* note 20, at 21–23.
[22] *Id*. at 23.
[23] UN Special Rapporteurs have a specific mandate from the Human Rights Council to monitor a specific human rights issue. *The Practical Guide to Humanitarian Law*, Medecins Sans Frontieres, https://guide-humanitarian-law.org/content/article/3/special-rapporteurs/.
[24] Lubin, *supra* note 20, at 14–15; Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37, 20 (Dec. 28, 2009) [hereinafter Countering Terrorism U.N. Report].

Rights and Fundamental Freedoms while Countering Terrorism specifically addressed the impact of state-led surveillance on human rights, expressing concern over states conducting unchecked surveillance and using prevention of terrorism as a catch-all exception to do so.[25] Similarly, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression condemned states' surveillance of social media users' activities as an impermissible infringement on the right to privacy.[26] Although states justified surveillance to protect national security and combat terrorism, in practice many states used surveillance for political ends to identify and target human rights defenders and members of the political opposition.[27] The same Special Rapporteur reiterated these concerns several years later, urging states to adopt national laws regulating surveillance to protect the right to privacy.[28] Based on the reports of the Special Rapporteurs, there was an emerging consensus that what constitutes an infringement on the right to privacy must adapt to the modern digital age.

B. Attention on the Right to Privacy Post-Snowden

A spotlight shone on the issue of the right to privacy and surveillance in the wake of the Snowden revelations. In June 2013, Edward Snowden, a former U.S. government contractor, revealed that the United States and the United Kingdom had created mass surveillance systems to monitor foreign nationals and their own citizens.[29] The revelations sent shockwaves throughout the international community, leading non-governmental and governmental organizations to take action to protect the right to privacy in the wake of this invasive surveillance.

Civil society reacted first in response to the Snowden revelations by publishing the International Principles on the Application of Human Rights to Communications Surveillance in 2014.[30] The Principles, created by a multi-stakeholder coalition of more than forty privacy and security experts,[31] guide states and non-state organizations to conduct surveillance and gather data in line with its thirteen principles. These principles include legality; legitimate aim; necessity; adequacy; proportionality; competent judicial authority; due process; user notification; transparency; public oversight; integrity of communications and systems; safeguards for international cooperation; safeguards against illegitimate access.[32] Since their publication, more than 400 organizations have adopted the Principles.[33]

---

[25] Countering Terrorism U.N. Report, *supra* note 24, at ¶¶ 20–22.
[26] Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27, ¶¶ 53–59 (May 16, 2011).
[27] *Id*.
[28] Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, summary (Apr. 17, 2013).
[29] Ewen Macaskill & Gabriel Dance, *What the revelations mean for you*, THE GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1; *Edward Snowden: Leaks that exposed US spy programme*, BBC (Jan. 17, 2013), https://www.bbc.com/news/world-us-canada-23123964.
[30] Electronic Frontier Foundation, *International Principles on the Application of Human Rights to Communications Surveillance* (May 2014), https://necessaryandproportionate.org/principles/ [hereinafter Civil Society International Principles].
[31] *Id.*
[32] *Id*.
[33] *Id*.

The UN was not far behind in its own response. The General Assembly and Human Rights Council began expressing increased concern over state surveillance, with the latter creating the Special Rapporteur on the Right to Privacy directly in response to the Snowden revelations in 2015.[34] The Special Rapporteur recommended the creation of "a legal instrument on surveillance and privacy" that contains "[a] set of principles and model provisions, to be integrated into national legislation."[35] The draft legal instrument, which was developed over a number of years but never passed, contained almost identical principles for states to follow as civil society's own Principles.[36] Since 2015, all bodies of the UN, and specifically the HRC, have year after year addressed concerns over state surveillance and the right to privacy as technology has grown more sophisticated.

III. The Exceptions Regime as it Applies to Privacy

The ICCPR always envisaged that a state party may restrict certain fundamental rights codified in the ICCPR in certain situations. The treaty explicitly creates an "Exceptions Regime" for certain rights in the text itself, permitting the party to impose restrictions on the right in the interest of protecting national security or another enumerated interest.[37] Although Article 17 does not create an explicit Exceptions Regime, one has been read into the ICCPR legal framework.[38] A closer examination of the legal basis of the Exceptions Regime and the Committee's application of the regime are essential to determining the precise requirements a state must meet when conducting surveillance for the sake of protecting national security.

A. Restricting ICCPR Rights and the Right to Privacy

Under the plain text of the ICCPR, a state may restrict the rights to liberty, public trial, expression, assembly, and association to protect national security subject to certain requirements.[39] The requirements to restrict are the same across these rights. A state may infringe on these "restrictable" rights if the measures taken are (1) prescribed by law; (2) for a legitimate state purpose in a democratic society, including to protect national security, public order or safety, or public health and morals; (3) necessary to pursue a legitimate purpose in a free and democratic society; (4) proportional, as enacted and implemented, to the risk of harm it seeks to avoid; and (5) consistent with "the fundamental principles of equality [before the law] and non-discrimination."[40]

---

[34] UN Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, A/HRC/37/62 (Oct. 25, 2018), ¶¶ 1, 10, 13.
[35] *Id.* at 16.
[36] *See Draft Legal Instrument on Government-led Surveillance and Privacy,* Version 0.6 (Jan.10, 2018), at 11–12, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf.
[37] ICCPR, *supra* note 3, arts. 12(3), 9, 14(1), 19(3)(b), 21, 22(2).
[38] *Id*., *supra* note 3, art. 17; Carrillo, *supra* note 3, at 647.
[39] ICCPR, *supra* note 3, art. 12(3), 9, 14(1), 19(3)(b), 21, 22(2).
[40] Carrillo, *supra* note 3, at 648 (citing Human Rights Comm., General Comment No. 27, ¶¶ 14, 18, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. 1) (Nov. 2, 1999); U.N. Counter-Terrorism Implementation Task Force, Basic Human Rights Reference Guide: Conformity of National Counter-Terrorism Legislation with International Human Rights Law, at 11, diagram 1.5 (Oct. 2014), https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/counterterrorismlegislation.pdf.

Article 17 contains an implicit Exceptions Regime because it only prohibits "*arbitrary* or *unlawful* interference" with a person's privacy.[41] In 1988, through GC 16, the HRC recognized the right to privacy's Exceptions Regime by providing definitions for what it means for an interference to be "unlawful" or "arbitrary."[42] Prohibition of unlawful interferences means that "no interference can take place except in cases envisaged by the law," and the law "itself must comply with the provisions, aims and objectives of the Covenant."[43] The Committee considers arbitrary inferences as those that are "provided for by law," but are not "reasonable under the particular circumstances."[44] Therefore, in the Committee's view in 1988, if there was a law in place and the interference was "reasonable," the interference was permitted.

The Committee enumerated further requirements for the legislation authorizing state interference with the right to privacy in GC 16. The enabling legislation "must specify in detail the precise circumstances in which such interferences may be permitted."[45] Additionally, any decision to authorize a measure that would infringe on the right to privacy "must be made only by the authority designated under the law, and on a case-by-case basis."[46] The HRC also created a general prohibition on the use of surveillance: "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[47]

However, in 2014, the Committee crafted a broader definition of "arbitrary." Although the new definition related to the prohibition of arbitrary detention under Article 9,[48] there is an understanding that this definition also applies to arbitrary interference under Article 17.[49] This new definition considers state action arbitrary when it "fails to guarantee due process and/or the other basic elements of '[justice], reasonableness, necessity and proportionality.'"[50] The Committee's Views post-2014 implement this new definition to disputes under Article 17, focusing on whether the interference of the right to privacy is in alignment with the principles of legality, necessity, and proportionality.[51]

B. Application of the Exceptions Regime to Surveillance

What compliance with the principles of legality, necessity, and proportionality means in practice requires examination of HRC jurisprudence and reports originating from other UN bodies, such as the Office of the United Nations High Commissioner for Human Rights and the Special

---

[41] ICCPR, *supra* note 3, art. 17 (emphasis added); Carrillo, *supra* note 3, at 647.
[42] GC 16, *supra* note 20, at ¶¶ 3, 4.
[43] *Id*. at 3.
[44] *Id.* at 4.
[45] *Id.* at 8.
[46] *Id.*
[47] *Id.*
[48] ICCPR, *supra* note 3, art. 9.
[49] Yuval Shany, *On-Line Surveillance in the case-law of the UN Human Rights Committee*, Federmann Cyber Security Research Center (July 13, 2017), https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee; *see also* Anja Seibert-Fohr, *Digital surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy* (April 25, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3168711.
[50] Carrillo, *supra* note 3, at 647 (citing Human Rights Comm., General Comment No. 35, 12, U.N. Doc. CCPR/G/GC/35 (Dec. 16, 2014)).
[51] Lubin, *supra* note 20, at 13, 15.

Rapporteur on the Right to Privacy. Satisfying the prong of legality is simple: a state must have some law in place that authorizes the interference with the right to privacy.[52] Committee Views and other UN materials reveal further requirements that the law authorizing surveillance for national security purposes must meet to satisfy the principles of necessity and proportionality: the legal framework must (1) specifically define the harm it seeks to prevent, (2) create an independent authorizing and oversight body, and (3) provide for transparency and individual remedies. Further, the government must (4) only carry out surveillance when there is a reasonable suspicion that the targeted individual will partake in the harm the state seeks to prevent, as provided for in the legislation, and (5) must balance the individual privacy and state interests to determine if the interference is reasonable in light of the circumstances.

1. Defines Harm

The law that authorizes the interference with the right to privacy must define the harm that it seeks to prevent. The mere existence of some justification is typically sufficient—the Committee subjects the interference to a balancing test against the justification at a later step in its analysis.[53] The ease of passing the "defines harm" threshold is evidenced in several HRC decisions. In *Madhewoo v. Mauritius*, the Committee was satisfied with the state's justification that it needed to expand the scope of legislation providing for the collection of fingerprints to prevent fraud.[54] In *Vandom v. Republic of Korea*, the Committee accepted Korea's public health justification for their mandatory HIV testing and reporting scheme for certain visa applicants.[55]

However, the Committee drew a line in the seminal case *Toonen v. Australia*, in which the claimant challenged a Tasmanian law criminalizing homosexuality.[56] The Tasmanian government posited that it sought to protect public health *and* public morals, arguing that public morals is a sufficient justification under the Article 17 exceptions regime.[57] While the HRC accepted that protection of public health may allow the state to interfere with the right to privacy, it rejected Tasmania's protection of morals justification.[58] The Committee held that protection of morals is an international concern and the growing consensus among states was to repeal laws criminalizing homosexuality.[59] Therefore, because there was no linkage between the protection of morals and Tasmania's law, the HRC conducted the rest of its analysis considering the public health justification only.[60] Although defining harm may be an easy hurdle to pass, there must be some rational connection between the intrusion and the harm.

2. Independent Authorization and Oversight

---

[52] UN Human Rights Council, The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights, OHCHR Annual Report A/HRC/39/29 (Aug. 3, 2018), ¶¶ 29, 34 [hereinafter OHCHR Annual Report on Privacy]; Sudalenko v. Belarus, CCPR/C/139/D/2929/2017 (Oct. 23, 2023), 7.5.
[53] *See* OHCHR Annual Report on Privacy, *supra* note 52, at ¶¶ 29, 34–38.
[54] Madhewoo v. Mauritius, CCPR/C/131/D/3163/2018 (Sept. 16, 2021), 7.5.
[55] Vandom v. Republic of Korea, CCPR/C/123/D/2273/2013 (July 12, 2018), 8.4.
[56] Toonen v. Australia, CCPR/C/50/D/488/1992 (March 31, 1994), ¶¶ 1, 2.1.
[57] *Id.* at 8.4.
[58] *Id.* at ¶¶ 8.5–8.6.
[59] *Id.* at 8.6.
[60] *See id.* at ¶¶ 8.1–8.7.

The law must create a system for judicial or regulatory authorization and oversight. The author in *Sudalenko v. Belarus* specifically complained that no judicial authority had ever authorized the Belorussian government's tracking of his movements in violation of Article 17.[61] Belarus could not contest this fact because it had no legal framework for its surveillance system; therefore, the Committee held that the state had violated the author's right to privacy in part because of the lack of authorization safeguards.[62] The HRC may also hold there has been a violation because the oversight is not sufficient in relation to the specific type of surveillance or data collection, as it did in *Madhewoo*.[63] Although Mauritius had some safeguards in place for collecting certain citizens' biometric information, it expanded its legislative authority to collect the data without creating a more robust oversight system.[64] Because the state did not provide for increased oversight and protection of this sensitive information, the Committee could not "conclude that there are sufficient guarantees against the risk of abuse and arbitrariness of the interference with the right to privacy."[65]

The decision in *Madhewoo* also suggests that the more sensitive the data collected is, the stronger the oversight system must be. Although Mauritius' oversight system was sufficient for other types of data, it no longer passed muster when the legislation expanded to collecting biometric data.[66] The European Court of Human Rights (ECtHR) decision in *Roman Zakharov v. Russia*, which many UN bodies draw on when discussing state surveillance and the right to privacy,[67] also contains this premise: more sensitive data collection and storage requires a proportionally more robust oversight system.[68]

Publications from the OHCHR clarify that the authorization and oversight systems must be independent of the legislature and independent of each other.[69] There must be independence at all stages of surveillance: when the measures are first ordered, when they are carried out, and after they have been terminated in order to protect any sensitive information collected.[70] Although a judicial body typically must authorize the surveillance, oversight may be carried out by a combination of administrative, judicial, and parliamentary bodies so long as they have "appropriate and adequate expertise, competencies and resources."[71]

3. Transparency and Individual Remedies

Surveillance legislation must be publicly accessible to ensure that the general public is aware of the potential use of surveillance against them and the remedies available to them.[72] This includes

[61] *Sudalenko*, *supra* note 52, at 3.3.
[62] *Id.* at 7.5
[63] *Madhewoo*, *supra* note 54, at ¶¶ 7.6–8.
[64] *Id.* at ¶¶ 2.2, 3.2.
[65] *Id.* at 7.6.
[66] *Id.*
[67] OHCHR Annual Report on Privacy, *supra* note 52, at 7 (citing Roman Zakharov v. Russia, application No. 47143/06, judgment of 4 December 2015); Report of the Special Rapporteur on the right to privacy, Human Rights Council, A/HRC/34/60 (March 2017) 56 (citing Roman Zakharov v. Russia).
[68] Roman Zakharov v. Russia, application No. 47143/06, judgment of 4 December 2015, ¶¶ 78, 191.
[69] OHCHR Annual Report on Privacy, *supra* note 52, at ¶¶ 39–40.
[70] *Id.* at 39 (citing CCPR/C/FRA/CO/5, 5).
[71] *Id.* at 40.
[72] *Id.* at ¶¶ 35, 58.

describing the "the nature of the offence and the category of persons that may be subjected to surveillance."[73] When no legislative framework exists, as was the case in *Sudalenko*, the author noted that because the government's ability to modify his data was not provided for by the law, he did not know "what measures he [could] take in order to ensure that his personal data [were] not modified compared to other citizens."[74] The Committee's View that Belarus had violated Sudalenko's right to privacy also focused on the lack of remedies available to him, stating that when a state collects an individual's data, Article 17 requires that the individual have the right to request rectification or deletion.[75] Because Belarus had no surveillance legislation in place at all, it could not dispute this lack of transparency or remedies.[76]

4. Reasonable Suspicion

If a state seeks to surveil an individual, it must have a reasonable suspicion that the individual will actually partake in the harm the state seeks to prevent; therefore, indiscriminate mass surveillance can never survive under the Article 17 Exceptions Regime, even if it is for the sake of protecting national security.[77] Part of the complainant's argument in *Sudalenko* drew on the state's apparent lack of reasonable suspicion that he posed any sort of threat.[78] Because the author was a law-abiding citizen and human rights defender, tracking his movements was "unnecessary in a democratic society."[79]

Although the HRC's View that Belarus had violated Sudalenko's Article 17 rights rested upon the lack of legislation and remedies,[80] it is highly likely that the HRC would have reached the same conclusion even if such law and remedies existed due to the lack of reasonable suspicion. The Special Rapporteur on the Right to Privacy has noted the ECtHR jurisprudence that developed the "reasonable suspicion" requirement for surveillance.[81] In *Zakharov v. Russia*, the ECtHR "unanimously held that the Russian system of secret interception of mobile telephone communications was a violation of article 8 of the [European Convention on Human Rights],"[82] which codifies the right to privacy.[83] Further, the ECtHR "accepted that, if certain conditions were satisfied, an applicant could claim to be a victim of a violation of article 8 owing to the mere existence of a secret surveillance measure."[84] From this case, the Special Rapporteur concluded that citizenship cannot serve as a proxy for "reasonable suspicion."[85]

---

[73] *Id.* at 35.
[74] *Sudalenko*, *supra* note 52, at 3.3.
[75] *Id.* at ¶¶ 7.4, 7.5.
[76] *Id.* at ¶¶ 7.4, 7.5.
[77] OHCHR Annual Report on Privacy, *supra* note 52, at 17 (citing A/HRC/33/29, 58; A/HRC/27/37, 25).
[78] *Sudalenko*, *supra* note 52, at ¶¶ 2.1, 3.3.
[79] *Id*.
[80] *Supra* Section III.B.1–3.
[81] Report of the Special Rapporteur on the right to privacy, Human Rights Council, A/HRC/34/60 (March 2017) ¶ 56.
[82] Report of the Special Rapporteur on the right to privacy, Human Rights Council, A/HRC/31/64 (2016), 36.
[83] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.
[84] Report of the Special Rapporteur on the right to privacy, Human Rights Council, A/HRC/31/64 (2016), 36.
[85] Report of the Special Rapporteur on the right to privacy, Human Rights Council, A/HRC/34/60 (March 2017) ¶ 56.

The OHCHR annual report implemented the holding in *Zakharov*, clarifying that indiscriminate mass surveillance "is not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures."[86] The OHCHR Report suggested that the "necessity" requirement is actually a requirement that the interference is necessary in a democratic society, and "[a]s the European Court of Human Rights has pointed out, 'a system of secret surveillance set up to *protect national security* may undermine or even destroy democracy under the cloak of defending it.'"[87] On proportionality, the mass surveillance system will fail because all individuals are subject to intrusive interference regardless of the level of potential threat they pose.

5. Reasonable in Light of the Circumstances: the Balancing Test

The Committee subjects a state's use of surveillance to a balancing test, weighing the individual's interest in the right to privacy against the state's interest in protecting whatever its surveillance system seeks to defend against. Based on HRC jurisprudence, it appears that the Committee conducts the same balancing test no matter what the state interest is, whether it is preventing crime (*Mahewoo*) or protecting public health (*Vandom* and *Toonen*).[88]

In *Madhewoo*, the Committee held that Mauritius had violated Article 17 because the broad scope of the data collection was unreasonable considering the legal protections in place.[89] The HRC took note of the "need to balance the protection of personal data with the pressing social need of preventing identity fraud," but the surveillance legislation in place to protect the collected biometric data was insufficient considering the "nature and scale of the interference."[90] The state policy created *mandatory* processing and recording of fingerprints; when the interference is this large scale, "it is essential to have clear, detailed rules governing the scope and application of measures" and to establish "minimum safeguards" covering the storage, duration of use, third party access, and procedures for destruction of the data to "provid[e] sufficient guarantees against the risk of abuse and arbitrariness."[91] Applying its test, Mauritius violated Article 17 in the Committee's view.[92]

Vandom and *Toonen* tested the application of the Article 17 balancing test to the state interest in protecting public health, but in these cases took issue with the underlying reasoning for the policies. In *Vandom*, the HRC concluded that the mandatory HIV testing policy that Korea imposed on visa applicants was not a reasonable restriction on several fronts.[93] First, the UNAIDS Secretariat's International Task Team on HIV-related Travel Restrictions found that HIV-related entry restrictions resulted in the unequal application of the law,[94] which cuts against the requirement that an ICCPR right may not be restricted inconsistently with the principles of

[86] OHCHR Annual Report on Privacy, *supra* note 52, at 17 (citing A/HRC/33/29, para. 58; A/HRC/27/37, para. 25).
[87] *Id.* at ¶¶ 10–11, 17 (citing Roman Zakharov v. Russia, para. 232) (emphasis added).
[88] *Madhewoo*, *supra* note 54, at ¶7.5; *Vandom, supra* note 55 at 8.9; *Toonen*, *supra* note 56 at 8.5.
[89] *Madhewoo*, *supra* note 54, at ¶¶ 7.5–7.6.
[90] *Id*.
[91] *Id.* at 7.6.
[92] *Id*.
[93] *Vandom, supra* note 55, at ¶¶ 8.2–9.
[94] *Id.* at 6.3.

equality before the law and non-discrimination.[95] Second, there was "no evidence demonstrat[ing] that HIV restrictions on entry, stay and residence based on positive HIV status alone serve to protect the public health;" in fact, the Committee pointed to evidence showing that such restrictions actually *harm* public health.[96] Third, the HRC noted that applying the testing requirement only to visa applicants alone was nonsensical if the policy was aimed to protect public health—it should apply to nationals and non-nationals alike.[97] The Committee reached the same conclusion in *Toonen* that the criminalization of homosexuality was not reasonable in relation to the state's interest in preventing the spread of HIV.[98] Again, no evidence existed that showed criminalizing homosexuality had any impact on mitigating HIV.[99]

Although there is no HRC jurisprudence conducting a balancing test with state surveillance to protect national security, the OHCHR suggested factors to consider.[100] To survive the balancing test, "[s]ecret surveillance measures must be limited to preventing or investigating the most serious crimes or threats" and "[t]he duration of the surveillance should be limited to the strict minimum necessary for achieving the specified goal."[101] The test should also consider the justifications for retaining and sharing the data, and the rules for both must be "clearly defined" and will be subjected to the same balancing test to determine their alignment with the principles of legality, necessity, and proportionality.[102] As the Committee noted in *Vandom*[103] and as the OHCHR noted in its report,[104] sometimes measures that seek to protect an interest actually harm it; therefore, the HRC will carefully scrutinize both the legal framework and practical application of state surveillance conducted to protect national security under this balancing test.

IV. Conclusions

This Article has detailed what ICCPR parties must do to conduct surveillance without violating Article 17. ICCPR parties must follow the Exceptions Regime established by international human rights law for restricting or limiting the enjoyment of fundamental rights, including privacy, when legislating and implementing measures of mass surveillance for legitimate state reasons, such as national security. This Exceptions Regime requires compliance with the principles of legality, necessity, and proportionality.

To conduct surveillance within the bounds of the Exceptions Regime, the state must have a legislative framework that defines the harm, creates independent authorization and oversight bodies, and provides for transparency and individual remedies. As shown by *Sudalenko*, in the absence of legislation, the Committee need not do much work to find an Article 17 violation. Without any law, the state has not publicly justified its surveillance system, the system is not legally subject to authorization or oversight, and there is no way for the public to know the

[95] *Supra* note 40 and accompanying text.
[96] *Vandom, supra* note 55, at ¶¶ 6.3, 8.9.
[97] *Id.* at 8.9.
[98] *Toonen*, *supra* note 56, at ¶¶ 8.5–8.6.
[99] *Id.* at 8.5–8.6.
[100] OHCHR Annual Report on Privacy, *supra* note 52, at 37.
[101] *Id.*
[102] *Id*.
[103] *Vandom, supra* note 55, at 8.9.
[104] OHCHR Annual Report on Privacy, *supra* note 52, at 17 (citing Roman Zakharov v. Russia, para. 232).

system exists or the remedies available to them if they have been surveilled. When legislation exists, like in *Madhewoo*, the HRC will consider if the legislation is robust enough in proportion to the interference—having some oversight is not sufficient if there is a high level of interference

If conducting surveillance for the sake of protecting national security, the state may only surveil individuals if it has a reasonable suspicion that the individual poses a national security threat, and the level of interference must be balanced against evidence that the interference will serve to protect national security. The Special Rapporteur has considered the reasonable suspicion requirement for conducting national security surveillance, noting that citizenship cannot serve as a proxy for a reasonable suspicion of terrorist activity.[105] Further, the Committee took issue in *Sudalenko* that Belarus surveilled a human rights defender with no criminal record—there was no suspicion that he posed any threat. In *Vandom* and *Toonen*, the Committee's balancing test was swayed by the lack of evidence that the interference with the individuals' privacy would achieve the states' goal to protect public health. The HRC will similarly require evidence to show that a surveillance system to protect national security will serve that purpose, especially considering the fear that a surveillance conducted to protect national security may ultimately undermine democracy.[106]

The question remains: what can be done about the current state of surveillance in Pakistan? This Article provides the framework that ICCPR parties must follow in an idealized state of following the HRC's non-binding recommendations. Its examination of ICCPR requirements reveals the specific ways that Pakistan is currently out of step with its obligation to protect citizens' right to privacy through its mass surveillance system: the laws, regulations and practices in place authorizing surveillance are unpredictable and minimal; the limited legislation does not provide for adequate oversight or remedies; and the surveillance is carried out indiscriminately against all of Pakistan's citizens. But conducting surveillance in alignment with Article 17 does not have to be all or nothing. By breaking down the individual components that bring a surveillance system into alignment with the ICCPR, this Article provides Pakistan (and all ICCPR parties), civil society, and individuals with ideas of the smaller steps that can be taken or advocated for to respect the right to privacy when engaging in national security surveillance.

[105] *See supra* note 85 and accompanying text.
[106] *See supra* note 86–87 and accompanying text.