List of Issues Submission to the United Nations Human Rights Committee During its Periodic Review of Kazakhstan

3 January 2022

We, Access Now, the International Justice Clinic at University of California, Irvine School of Law, MediaNet, and Public Association Dignity, jointly submit to the Human Rights Committee ("you" or the "Committee") this written contribution for adoption of the List of Issues Prior to Reporting (LOIPR) of the third cycle of periodic review on Kazakhstan.

This submission informs the Committee of two important emerging issues of Kazakhstan's non-compliance with the International Covenant on Civil and Political Rights (ICCPR): internet shutdowns, and the use of spyware against human rights defenders, journalists, and government critics, which we recommend you to include in the LOIPR.

Information on Submitters

Access Now, a United Nations Economic and Social Council (ECOSOC) accredited organization, routinely engages with the United Nations (UN) in support of our mission to extend and defend the digital rights of users and communities at risk around the world.[1] Since its founding in 2009, Access Now has monitored the abuse and misuse of new and emerging technologies in ways that threaten the realization of fundamental human rights, including the freedoms of expression, association, and peaceful assembly, and the rights to privacy and non-discrimination. Access Now closely monitors internet shutdowns and other intentional disruptions to internet access, and coordinates the global #KeepItOn coalition and campaign against internet shutdowns.[2]

The International Justice Clinic at the University of California, Irvine School of Law, produces research and conducts advocacy promoting compliance with international human rights law and,

[1] Access Now, *About Us*, 2023.
[2] Access Now, *#KeepItOn*, 2023.

inter alia, UN human rights mechanisms.[3] Since its founding in 2012, under the direction of Professor David Kaye, a former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Clinic has continuously researched and advocated for freedom of expression and privacy. Supported by the Clinic, Prof. Kaye recently testified on the human rights impact caused by spyware before the European Parliament's PEGA Committee.[4]

MediaNet International Centre for Journalism is a non-governmental organization founded by Kazakhstani journalists in 2004.[5] The organization works on developing civil society in Kazakhstan and other Central Asian countries by strengthening the potential and capacities of independent mass media. MediaNet supports public organizations and defends human rights and fundamental freedoms. In the last two years, MediaNet campaigned for freedom of expression on the internet.

Public Association Dignity (Қадір-қасиет) was founded on 1 September 2010 in Astana, Kazakhstan, to promote the observance of human rights and freedoms and the development of civil society; to analyze legislation for compliance with international standards; and to engage in education and advocacy.[6] Among the five main areas of the organization's activity are: the security of human rights defenders, including information and digital threats; the implementation of decisions of UN committees; the presumption of innocence; the right of the child to protection from bullying and cyberbullying; and the right of women to participate in state affairs.

Information on Kazakhstan's non-compliance with the Covenant

Use of internet shutdowns during elections, protests, and other critical events

Summary

Kazakhstan has repeatedly denied access to the internet, including by throttling and blocking websites, since 2016, particularly during important events, such as elections and protests, where individuals exercise fundamental human rights. In 2018, 2019, and in 2021 authorities hit the 'kill switch' - denying complete access to the internet - during anti-government protests in order to disrupt opposition political activities. The most serious internet blackout to date was implemented by Kazakhstan's authorities in January 2022, amidst widespread protests over the government's lifting of the liquefied petroleum gas price cap.

Relevant Articles of ICCPR

Articles 2(1) and (3), 19(2) and (3), 21

[3] The International Justice Clinic, *About the Clinic*.
[4] David Kaye, *Testimony to the PEGA Committee of the European Parliament, the impact of spyware on fundamental rights*, 27 October 2022. You can find out about the Clinic's other work at https://ijclinic.law.uci.edu/.
[5] MedieNet, *About MediaNet*.
[6] Public Association Dignity, *О Нас*.

Prior Recommendations by the Committee

- In its 2011 Concluding Observations,[7] the Committee expressed concern about Kazakhstan's noncompliance with Article 19 of the ICCPR and recommended Kazakhstan ensure the free exercise of the right to freedom of expression by journalists, human rights defenders, and individuals (para. 25). Disappointingly, Kazakhstan did not provide any information on measures taken to comply with the recommendation.[8] In its 2016 Concluding Observations,[9] the Committee reiterated its concern about Kazakhstan's noncompliance with Article 19, especially its "blocking of social media, blogs, news sites and other Internet-based resources on national security grounds, including by using Law No. 200-V of 23 April 2014, which entrusts the Prosecutor General or his deputies with the ability to shut down or suspend a network or means of communication and access to Internet resources without a court order" (para. 49), and recommended Kazakhstan repeal or otherwise revise legal provisions limiting freedom of expression (para. 50(b)).
- The Committee expressed its concerns in the 2011 (para. 26) and 2016 Concluding Observations (paras. 51 and 52) about Kazakhstan's non-compliance with Article 21 and recommended Kazakhstan revise all relevant regulations, policies, and practices to ensure any restrictions on freedom of assembly.

Kazakhstan's current law, policies, and practices

Law authorizes blanket internet shutdowns without court order

Despite the recommendations in the Committee's 2016 Concluding Observations (paras. 50(b) and 52), Kazakhstan has failed to repeal or revise the Law on Communications (Law No. 200-V of 23 April 2014). Article 41-1 of the law allows the General Prosecutor or his deputies to order an internet shutdown or website throttling or blocking without a court order if the General Prosecutor finds calls for extremist and terrorist activities, mass riots, as well as participation in mass (public) activities conducted in violation of the established procedure.[10] To date, this law still authorizes Kazakhstan to implement internet shutdowns and website throttling and blocking as below.

Internet shutdowns implemented by Kazakhstan

Authorities in Kazakhstan have implemented website blockings since 2016, particularly during critical political moments such as elections and protests where individuals exercise fundamental human rights. In March 2021, authorities shut down the internet in an effort to stop

[7] Human Rights Committee, Concluding Observations on Kazakhstan, CCPR/C/KAZ/CO/1,19 August 2011.
[8] Fabián Omar Salvioli, the Special Rapporteur for Follow-up to Concluding Observations of the Human Rights Committee, Follow-up letter sent to the State party, 2 December 2013.
[9] Human Rights Committee, Concluding Observations on Kazakhstan, CCPR/C/KAZ/CO/2, 9 August 2016.
[10] Law No. 200-V, 23 April 2014. Unofficial English translation is available at https://adilet.zan.kz/eng/docs/Z040000567_.

anti-government protests,[11] and throttled social media in March 2019[12] and in 2018[13] to disrupt opposition political activities.

The most serious internet blackout to date was implemented by Kazakhstan's authorities in January 2022, amidst widespread protests over the government's lifting of the liquefied petroleum gas price cap, which led to deadly state violence in Almaty and across Kazakhstan.[14]

The scale and the impact of the January 2022 shutdowns were unprecedented.[15] For more than a week, Kazakhstan authorities arbitrarily manipulated and disrupted internet access across the country, leaving much of the population disconnected and uncertain about whether or when the internet will be fully accessible. Access Now and partners have documented the timeline of the shutdowns, with more limited disruptions happening between January 2 and 3, and full internet blackouts taking place between January 4 and 7.[16] Smaller disruptions continued to happen up until January 17.[17]

The blackouts left people in Kazakhstan in a state of fear and confusion. The shutdowns adversely affected the country's residents and its businesses; disruptions in mobile payments services and the functioning of debit card machines caused cash and food shortages.[18]

The government also disrupted the media's ability to report on the events, affecting local media websites and blocking independent outlets such as Orda.kz and kaztag.kz, while limiting international media's ability to connect with people on the ground.[19] The media blackout was so extensive that some people were not even aware the Collective Security Treaty Organization (CSTO) troops had been deployed in their country. President Kassym-Jomart Tokayev, in his address to the people of Kazakhstan on January 7, 2022, admitted that the government implemented the shutdowns, adding that "free access to the internet does not mean free publication of fabrications, slander, insults, and inflammatory appeals."[20]

---

[11] Access Now, *Civil society reports internet shutdowns in two cities in Kazakhstan during February 28 protests*, 10 March 2021.
[12] Access Now, *Targetted, Cut off, and Left in the Dark, The #KeepItOn Report on Internet Shutdowns in 2019*, page 10.
[13] Access Now, *The State of Internet Shutdowns around the World, The 2018 #KeepItOn Report*, page 12.
[14] Access Now, *Timeline: Kazakhstan internet shutdowns aim to crush protests, hide state violence*, 12 January 2022.
[15] Forbes, *Интернет по расписанию и отключения вручную: как блокируют связь в Казахстане*, 11 January 2022.
[16] Access Now, *Timeline: Kazakhstan internet shutdowns aim to crush protests, hide state violence*, 12 January 2022.
[17] Access Now, *#KeepItOn: people in Kazakhstan have the right to internet access*, 17 January 2022.
[18] Thomson Reuters Foundation News, *ANALYSIS-Kazakhstan's internet shutdown leaves millions in the dark during unrest*, 10 January 2022; New York Times, *Kazakhstan's Internet Shutdown Offers Lessons for Russia-Ukraine Crisis*, 18 February 2022; and Eurasianet, *Food and cash shortages spread as Kazakhstan throttles internet. Modern life falls apart without an internet*, 8 January 2022.
[19] Cloudflare, *Internet shut down in Kazakhstan amid unrest*, 5 January 2022; and Власть, *Сайты КазТАГ и Orda.kz заблокированы на фоне освещения протестов*, 4 January 2022.
[20] The Republic of Kazakhstan, *President Kassym-Jomart Tokayev's address to the people of Kazakhstan*, 7 January 2022.

Despite the government's attempt to use shutdowns to hide its abusive actions toward its own people, a year after the "January events," as they are now known in Kazakhstan, the deaths and abuses that happened are public knowledge. At least 238 people died as a result; over 4,000 injured; nearly 12,000 detained; at least 1,113 people convicted (this includes only one government official); and some protesters have been allegedly tortured to elicit forced confessions.[21] One year later, according to Human Rights Watch, "the government has taken no good faith steps to identify the law enforcement officers responsible and hold them to account."[22]

As the government of Kazakhstan faces no accountability, it continues the abuses. The #KeepItOn coalition received reports of internet shutdowns before and after the 20 November 2022 extraordinary presidential elections, to suppress information and protests. This included targeted blocking of social media and communications platforms such as YouTube, Twitter, Telegram, Instagram, and Signal, as well as preventing access to certain websites prior to the polls opening.[23] On November 1, there was an apparent internet disruption that the government claimed was due to investigation of cyber attacks.[24]

After the election, as authorities inaugurated the president on November 26, protestors on the streets of Astana were met with another internet shutdown.[25]

The Committee's General Comments, other United Nations bodies' recommendations, and other international norms

Kazakhstan's internet shutdowns and website blockings as well as the law which authorizes these conducts violates Articles 19(2),(3) and 21

The Committee in General Comment 34 stated that: Article 19(2) protects "internet-based modes of expression;"[26] any restrictions on the operation of websites, blogs or social media websites must meet a stringent standard under Article 19(3);[27] and internet shutdowns and website throttling or blockings are per-se disproportionate ("permissible restrictions generally should be content-specific and generic bans on the operation of certain sites and systems are

[21] The Diplomat, *Curious Case of the Kyrgyz Jazzman Detained in Kazakhstan*, 11 January 2022; Republic World.com, *Kazakhstan Unrest: Nearly 225 People Killed, Over 4500 Injured During Violent Protests*, 16 January 2022; and Human Rights Watch, *Kazakhstan: No Justice for January Protest Abuses*, 20 December 2022.
[22] *See* Human Rights Watch, *supra* note 21.
[23] Inform Buro, *В Казахстане не работают YouTube, Telegram, Instagram и Facebook*, 21 October 2022; Экспресс К, *Казахстанцы стали жаловаться на сбои в работе Instagram*, 30 October 2022; and *Another potential #InternetShutdown in the EE/Central Asia region tonight*, Twitter, 29 October 2022.
[24] Inform Buro, *Почему у казахстанцев плохо работает интернет, объяснил Мусин*, 1 November 2022.
[25] Власть о главном, *В Астане перебои с интернетом - и мобильным и стационарным, сообщают корреспонденты Власти в городе*, Telegram, 26 November 2022.
[26] Human Rights Committee General Comment No. 34: Article19: Freedom of opinion and expression, CCPR/C/GC/34, 12 September 2011, para. 12.
[27] *Id.* at para. 43.

not compatible with paragraph 3").[28] It also stated that prohibition of a website "solely on the basis that it may be critical of the government or the political social system" is inconsistent with Article (3).[29] The Committee also recently expressed its concerns about internet shutdowns in Ethiopia in its Concluding Observations, especially their nonconformity with the proportionality test under Article 19(3).[30]

The Committee clarified in General Comment 37 that Article 21 protects peaceful assemblies both on and offline,[31] including "mobilization of resources; planning; dissemination of information about an upcoming event; preparation for and traveling to the event; communication between participants leading up to and during the assembly; broadcasting of or from the assembly; and leaving the assembly afterwards;"[32] and its restriction is subject to the strict standard which is equivalent to the one Article 19(3) requires.[33]

In response to the 2022 January internet shutdown, then UN High Commissioner for Human Rights, Michelle Bachelet, underlined that shutting down the internet "is not the answer to a crisis but risks fueling the violence and unrest" and urgently appealed for internet access in Kazakhstan to be "immediately and completely restored."[34]

The current law in Kazakhstan violates Articles 19(2),(3) and 21 for two reasons. First, it authorizes the government to implement blanket internet shutdowns and website throttling or blocking which are incompatible with the Covenant. It is especially concerning that the law authorizes internet shutdowns due to unauthorized public gatherings because Kazakhstan often abuses national security and public order grounds to ban protests.[35] Second, the Communications Act permits an internet shutdown under the vague condition that the authorities find calls for extremist and terrorist activities, mass riots, as well as participation in mass (public) activities conducted in violation of the established procedure, which does not provide for the specificity required by the General Comment 34.

---

[28] *Id*. *See also* Report of the Special Rapporteur on peaceful assembly and of association, A/HRC/47/24/Add.2, 15 June 2021, para. 44 (attempts to tackle problems such as disinformation and hate speech cannot justify "internet shutdowns, which are disproportionate by default, and should strictly adhere to international human rights principles and standards, including those concerning the right to freedom of expression").
[29] *Supra* note 26, para. 42.
[30] Human Rights Committee, Concluding Observation on Ethiopia, CCPR/C/ETH/CO/2, 7 December 2022, para. 39.
[31] Human Rights Committee, General Comment No. 37 on the right of peaceful assembly (article 21), CCPR/C/GC/37, 17 September 2020, para. 6.
[32] *Id*. at para. 33.
[33] *Id.* at paras. 36-69.
[34] UN News, *UN urges restraint in Kazakhstan, with dozens reportedly killed*, 6 January 2022.
[35] Concluding Observations on Kazakhstan (2016), *supra* note 9, para. 51 (The Committee expressed concern about the imposition of penalties for "providing 'assistance' to 'illegal' assemblies."). *See also* Freedom House, *Kazakhstan: Authorities Rush to Further Limit Peaceful Assembly*, May 4, 2020; and Radio Free Europe/Radio Liberty, *Kazakh Authorities Detain Activists In Apparent Bid To Halt Protests On Country's Independence Day*, 16 December 2022.

Kazakhstan has been failing to investigate the shutdowns and the associated abuses, including deaths, injuries, and arbitrary convictions and detentions, violating Article 2(3)

The Human Rights Committee stated in General Comment 31 that states are obliged to "investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies";[36] if the violations are revealed, to provide "accessible and effective remedies" to victims,[37] "take measures to prevent a recurrence of a violation,"[38] and "ensure that those responsible are brought to justice."[39] The Committee further stated that failure to meet these obligations constitutes a separate violation of the Covenant.[40]

Kazakhstan has been failing to discharge these obligations with respect to internet shutdowns in 2022 as well as website blocking and throttling in 2018, 2019, and 2021.

Recommended questions to be included in the List of Issues Prior to Reporting

- What steps will Kazakhstan take, and when will it take them, to bring its legislation, especially the Law on Communications (Law No. 200-V of 23 April 2014), into compliance with Articles 19(2),(3) and 21 of the Covenant?
- How and when will Kazakhstan investigate the 2022 internet shutdowns as well as those in 2018, 2019, and 2021, hold those responsible accountable, provide meaningful remedies to the people affected, and ensure non-repetition?
- How will Kazakhstan prevent internet shutdowns, and blocking and throttling of websites, which are incompatible with the Covenant?

Suggested recommendations to be included in the Concluding Observations

- Review and revise the Law on Communications (Law No. 200-V of 23 April 2014) so that it complies with Articles 19(2),(3) and 21;
- Thoroughly investigate the 2022 internet shutdowns as well as those in 2018, 2019, and 2021, hold the responsible individuals accountable, and provide remedies to the people affected so that it complies with Article 2(3);[41] and
- Take all effective steps necessary to end shutdowns, throttling, or blocking of the internet or websites, especially during elections, protests, and other important events for individuals to exercise their fundamental human rights so that it complies with Articles 2(1), 19(2),(3) and 21, including by working with the internet service providers.[42]

---

[36] Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13, 26 May 2004, para. 15.
[37] *Id.*
[38] *Id*. at para. 17.
[39] *Id*. at para. 18.
[40] *Id*.
[41] *See* The Supreme Court of India, *Anuradha Bhasin v. Union of India*,10 January 2020, para. 152(g).
[42] *See* The Community Court of Justice of the Economic Community of West African States (ECOWAS Court), *SERAP v. Federal Republic of Nigeria*, 14 July 2022, para. 102; and ECOWAS Court, *Amnesty International Togo and Ors v. The Togolese Republic*, 25 June 2020, para. 47(v).

Use of spyware against journalists, human rights defenders, and government critics

Summary

Despite the Committee's recommendations, Kazakhstan continues threatening, assaulting, and harassing journalists, human rights defenders, and government critics. Since 2016, Kazakhstan has been reportedly deploying spyware against such individuals, while failing to admit its use of spyware or even investigate the alleged spyware abuses. This failure is causing the people of Kazakhstan to fear retaliation by the government, producing a severe chilling effect on the exercise of fundamental human rights.

Relevant Articles of ICCPR

Articles 2(1) and (3), 17(1), 19, 21, 22

Prior Recommendations

- The Committee, in its 2011 Concluding Observations,[43] expressed concerns about the threats, assaults, harassment, and intimidation of journalists and human rights defenders and recommended Kazakhstan to ensure that those are able to freely exercise the right to freedom of expression (para. 25). Disappointingly, Kazakhstan did not provide any information on measures taken to comply with the recommendation.[44] The Committee, in its 2016 Concluding Observations,[45] expressed its concerns about interference with professional journalistic activity such as shutting down of independent newspapers and magazines, television channels, and news websites for reportedly minor irregularities or on extremism related charges (para. 49) and recommended Kazakhstan to review its law to conform with Article 19, including its Law No. 200-V of 23 April 2014, which enables authorities to access to internet resources without a court order (para. 49), and recommended Kazakhstan repeal or otherwise revise legal provisions limiting freedom of expression (para. 50).
- The Committee also stressed concern in the 2011 (para. 26) and 2016 Concluding Observations (paras. 51 and 52) about Kazakhstan's non-compliance with Article 21.
- The Committee also stressed concern in the 2011 (para. 27) and 2016 Concluding Observations (paras. 53 and 54) about Kazakhstan's non-compliance with Article 22.

Kazakhstan's current policy and practices

Spyware is a type of malicious software secretly installed on devices that enables covert surveillance of users by monitoring, extracting, or analyzing data from such devices. Some of the most sophisticated types of spyware, such as Pegasus, made by the Israeli company NSO Group[46] or Hermit, made by the Italian RCS Lab,[47] can be installed remotely without any action of a victim, and once installed, they allow an attacker to take full control of the device. As a result of private vendors' global sales of spyware, governments' use of spyware—including

[43] Concluding Observations on Kazakhstan, s*upra* note 7.
[44] Follow-up letter sent to the State party, *supra* note 8.
[45] Concluding Observations on Kazakhstan, *supra* note 9.
[46] The Guardian, *The Pegasus project*.
[47] Lighthouse Reports, *Revealing Europe's NSO*, 28 August 2022.

against journalists, human rights defenders, and critics—is proliferating on a global level, causing a deep chilling effect on individuals' exercise of fundamental human rights.

In 2016, the government of Kazakhstan evidently used spyware against members of Respublika—an independent newspaper which a court in Kazakhstan ordered to shut down in 2012[48]—and their family members as well as their attorneys, one of whom was an opposition party Democratic Choice of Kazakhstan.[49]

In 2021, Amnesty International's Security Lab confirmed the phones of at least four Kazakh human rights activists from Oyan, Qazaqstan! (Kazakh for "Wake up, Kazakhstan!"),[50] were infected with Pegasus spyware.[51] In addition, more than a dozen journalists, activists, politicians of opposition parties, and businesspersons were at least potentially targeted, according to the Pegasus Project investigation.[52]

In April 2022, according to the cyber security research group Lookout, only four months after the January 2022 nationwide protests, Kazakhstan reportedly used Hermit spyware against undisclosed victims.[53]

Unlike other countries which are investigating and trying to hold those responsible for the abuse of spyware accountable,[54] such as the United States,[55] the European Union,[56] India,[57] or France,[58] Kazakhstan has failed to take measures to investigate or even acknowledge its use of

---

[48] Eurasianet, *Kazakhstan: Court Bans Outspoken Newspaper amid Political Crackdown*, 25 December 2012. In 2016, the Human Rights Committee showed its concern about the shutdown of independent newspapers in its Concluding Observations (Concluding Observations on Kazakhstan, s*upra* note 9, para. 49).

[49] The Electronic Frontier Foundation, *Malware Linked to Government of Kazakhstan Targets Journalists, Political Activists, Lawyers: EFF Report*, 4 August, 2016.

[50] Oyan, Qazaqstan! is a youth movement organization established in 2019 after the resignation of long-time President Nursultan Nazarbayev and has been organizing demonstrations, civil rights walks, and art performances of protest. *See* Global Voices, *'Our activism won't stop': The Oyan movement recounts the January protests in Kazakhstan*, 14 January 2022.

[51] Amnesty International, *Kazakhstan: Four activists' mobile devices infected with Pegasus Spyware*, 9 December 2021.

[52] Amnesty International, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*, 19 July 2021; and Organized Crime and Corruption Reporting Project, *A World of Surveillance*.

[53] Lookout, *Lookout Uncovers Hermit Spyware Deployed in Kazakhstan*, 16 June 16 2022.

[54] *See* Citizen Lab, *Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry*, 7 December 2022.

[55] The New York Times, Lawmakers Signal Inquiries Into U.S. Government's Use of Foreign Spyware, 28 December 2022; U.S. House of Representatives Permanent Select Committee on Intelligence, House Intelligence Committee Open Hearing on Commercial Cyber Surveillance, 27 July 2022; and U.S. Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, 3 November 2021.

[56] Committees European Parliament, *Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware*.

[57] The Supreme Court of India, *Manohar Lal Harma v. Union of India and Ors*, 27 October 2021.

[58] Reporters Without Borders, *Pegasus judicial proceedings in France offer only possibility of justice*, 18 July 2022.

spyware, despite the allegations that even the current president, Kassym-Jomart Tokayev, has been a potential target himself.[59]

In addition to the use of spyware, Kazakhstan's multiple attempts to force people in Kazakhstan to install government "national security certificates" on digital devices—which enables Kazakhstan to intercept encrypted traffic and significantly weakens online security for individuals in Kazakhstan—show its total disregard for the right to privacy.[60]

The Committee's General Comments and other United Nations bodies' recommendations

Kazakhstan's use of spyware violates the Covenant

The Human Rights Committee has stated in General Comment 34[61] that Article 19(1) guarantees the right to maintain opinions without interference, and as such, it permits no exception or restriction. Spyware would interfere with this absolute right, given that spyware disincentives individuals to freely conduct research or communicate with others through mobile or computer devices, which are quintessential to form and hold opinions.

The actual and potential use of spyware interferes with the rights to privacy, freedom of expression, peaceful assembly, and association. The Committee has stated in General Comment 16[62] and Views in *Toonen v. Australia*,[63] General Comment 34,[64] and 37,[65] and Views in *Vladimir Romanovsky v. Belarus* (para. 7.2)[66] that the rights to privacy, the rights to freedom of expression, peaceful assembly, and association allow for interference in exceptional cases where a state has shown that the prescribed conditions are met, i.e., legality, legitimacy, and necessity and proportionality. The Committee also stated in Views of *Madhewoo v Mauritius* (paras. 7.4) that Article 17(1) requires strict safeguards in place which sufficiently eliminate the risk of arbitrary interference.[67]

The Committee expressed its concerns about states' use of spyware, and the lack of sufficient safeguards in particular in past Concluding Observations on other states.[68] But beyond that, a

---

[59] Organized Crime and Corruption Reporting Project, *Kassym-Jomart Tokayev Politician or Government Official - Kazakhstan*.
[60] ZDNET, *Kazakhstan government is intercepting HTTPS traffic in its capital*, 6 December 2020; Global Voices, *Kazakhstan pauses interception of encrypted traffic, but for how long?*, 30 August 2019; and ZDNET, *Kazakhstan will force its citizens to install internet backdoors*, 3 December 2015.
[61] General Comment No. 34, *supra* note 26, para. 9.
[62] Human Rights Committee General Comment No. 16 (1988): Article 17 (Right to Privacy), CCPR/C/GC/16, 8 April 1988, paras. 3 and 7.
[63] Human Rights Committee, *Toonen v. Australia*, CCPR/C/50/D/488/1992, 31 March 1994, para. 8.3.
[64] General Comment No. 34, *supra* note 26, para. 37.
[65] General Comment No. 37, *supra* note 31, para. 36.
[66] Human Rights Committee, *Vladimir Romanovsky v. Belarus*, CCPR/C/115/D/2011/201, 7 December 2015, para. 7.2.
[67] Human Rights Committee, *Madhewoo v Mauritius*, CCPR/C/131/D/3163/2018, 21 July 2021, paras. 7.4 and 7.6.
[68] *See* Human Rights Committee, Concluding Observation on Germany, CCPR/C/DEU/CO/7, 30 November 2021, paras. 42 and 43; Concluding Observation on Netherlands, CCPR/C/NLD/CO/5, 22 August 2019, paras. 54 and 55; Concluding Observation on Italy, CCPR/C/ITA/CO/6, 1 May 2017, paras 36 and 37.

strong case can be made that *any* use of spyware, especially with equivalent characteristics to Pegasus, cannot satisfy these requirements of Article 17, 19(2)(3), 21 and 22 for two reasons.[69] First, spyware such as Pegasus allows indiscriminate and virtually complete access to data and recording functions on a target's device, likely making it impossible to meet the proportionality principle. Second, it is currently questionable whether the design and implementation of safeguards which satisfy the standards under Article 17(1) would be practically possible to implement.

The General Assembly and the Human Rights Council have repeatedly stated that states should refrain from unlawful or arbitrary surveillance, including by way of hacking; establish independent oversight mechanisms; and provide victims with access to an effective remedy.[70] Further, in 2021, multiple UN experts called for a global ban of the sale and transfer of spyware.[71]

Lack of investigation

The Human Rights Committee stated in General Comment 31 that states are obliged to "investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies," and if the violations are revealed, to provide "accessible and effective remedies" to victims, "take measures to prevent a recurrence of a violation," and "ensure that those responsible are brought to justice." The Committee further stated that failure of these obligations constitute a separate violation of the Covenant.

Kazakhstan has been failing to discharge these obligations with respect to the alleged spyware infections and targeting of individuals under its jurisdiction.

Recommended questions to be included in the List of Issues Prior to Reporting

- How and when will the government of Kazakhstan investigate the use of spyware, hold the responsible accountable, provide meaningful remedies to people affected, and ensure non-repetition?
- How and when will the government of Kazakhstan end the use of spyware, which is incompatible with the Covenant, especially against journalists, human rights defenders, and government critics?

[69] *See* David Kaye, *supra* note 4, para. 15.
[70] General Assembly resolutions, The right to privacy in the digital age, A/RES/77/211, 15 December 2022 and A/RES/75/176, 28 December 2020; and Human Rights Council resolutions, Right to privacy in the digital age, A/HRC/RES/48/4, 13 October 2021. Further, in 2022, Human Rights Council expressed concerns about the use of spyware in various resolutions, i.e., The promotion and protection of human rights in the context of peaceful protests; A/HRC/RES/50/21, 14 July 2022; Recognizing the contribution of human rights defenders, including women human rights defenders, in conflict and post-conflict situations, to the enjoyment and realization of human rights, A/HRC/RES/49/18, 8 April 2022; and Situation of human rights in Myanmar, A/HRC/RES/49/23, 8 April 2022.
[71] The Office of the High Commissioner for Human Rights, *Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech*, 12 August 2021.

Suggested recommendations to be included in the Concluding Observations

- Ban, or at least implement a moratorium on the use of spyware, especially those with functions equivalent to Pegasus spyware until Kazakhstan designs and implements safeguards that can effectively prevent any abuse of spyware to meet the requirement of Article 17(1).[72] Such safeguards include:
    - judicial pre-approval;[73]
    - effective and independent oversight which:[74]
        - monitors every process of each spyware use, including judicial pre-authorization, actual spyware use, and termination of the use;
        - investigates alleged use of spyware, which violates Article 17, 19, 21, and 22;
        - publicly discloses the result of such oversight for public scrutiny;
    - prohibition of data sharing and data repurposing;[75] and
    - prohibition of use of evidence which is directly or indirectly obtained through the misuse of spyware.[76]
- Stop using spyware and other forms of invasive surveillance against journalists, activists, human rights defenders, and government critics, to comply with Articles 17, 19, 21, and 22.
- Investigate such uses of spyware and hold responsible individuals accountable, and provide access to effective remedies to people affected, including providing ex-post notification to all individuals against whom spyware is used so that they can exercise the right to remedy, to comply with Article 2(3).[77]

[72] *See* European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, *Draft Report*, 8 November 2022, para. 586. *See also*, David Kaye, *Here's what world leaders must do about spyware*, Committee to Protect Journalists, 13 October 2022; and Access Now, *The Geneva Declaration on Targeted Surveillance and Human Rights*, 29 September 2022.
[73] *See* Concluding Observations on Italy, *supra* note 68, para. 37. *See also*, The Office of the High Commissioner for Human Rights, *The right to privacy in the digital age* (2018), A/HRC/39/293, August 2018, para. 39 ("[the judicial branch] needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary, and proportionate and authorize (or reject) ex ante the surveillance measures"); and The right to privacy in the digital age (2014), A/HRC/27/37, 30 June 2014, para. 30.
[74] *See* Human Rights Committee, Concluding Observations on Macao, China, CCPR/C/CHN-MAC/CO/2, 27 July 2022, para. 33; Human Rights Committee, Concluding Observations on Georgia, CCPR/C/GEO/CO/5, 13 September 2022, para. 40. *See also*, The Office of the High Commissioner for Human Rights, The right to privacy in the digital age (2018), *supra* note 73, paras. 39 and 40; The right to privacy in the digital age (2014), *supra* note 73, paras. 37 and 38.
[75] *See Madhewoo v Mauritius*, *supra* note 67, paras. 7.4 and 7.6; Human Rights Committee, Concluding Observations on Canada, CCPR/C/CAN/CO/6, 13 August 2015, "c. Counter-terrorism."
[76] *See* Human Rights Committee, General Comment No. 20: Article 7 (Prohibition of torture, or other cruel, inhumane or degrading treatment or punishment), 10 March 1992, para. 12.
[77] *See* Concluding Observations on Italy, *supra* note 68, para 37; Human Rights Committee, Concluding Observations on Poland, CCPR/C/POL/CO/7, 23 November 2016, paras. 39 and 40; and Concluding Observations on Ukraine, CCPR/C/UKR/CO/8, 9 February 2022, para.42.

Thank you very much for your consideration. If you have any questions on this submission, please contact Hinako Sugiyama, Digital Rights Fellow (hsugiyama@law.uci.edu) at the International Justice Clinic, the University of California, Irvine School of Law.