Privacy International's response to the call for input for a thematic study by the UN Working Group on Enforced or Involuntary Disappearances on "new technologies and enforced disappearances"

February 2023

Introduction

Privacy International (PI) welcomes the opportunity to provide input to the thematic study by the Working Group on Enforced or Involuntary Disappearances on "new technologies and enforced disappearances".

Privacy International (PI) is a non-governmental organisation that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights and the UN Refugee Agency.

The following sections provide PI's information and analysis of some of the topics listed in the call for submission.[1] The widespread use of new technologies presents both opportunities and challenges for the protection of human rights, including the right to life and the right to privacy. It is essential that states take a human rights-centered approach in their use of these technologies, and ensure that their use is consistent with international human rights law. By doing so, states can ensure that new technologies are used to enhance the protection of human rights, rather than to facilitate the commission of human rights violations. In the following submission, first, we highlight how the use of new technologies to facilitate enforced or involuntary disappearances. Second, we raise our concerns on it is increasingly clear that some states are using the guise of protecting against enforced disappearances as a pretext to introduce broad and overreaching surveillance measures.

[1] Call for inputs for a thematic study by the Working Group on Enforced or Involuntary Disappearances on "new technologies and enforced disappearances", https://www.ohchr.org/en/calls-for-input/2023/call-inputs-thematic-study-working-group-enforced-or-involuntary

We recommend the Working Group on Enforced or Involuntary Disappearances to include the following recommendations in its report:

- To highlight the obligation of states to conduct investigations of enforced disappearances in accordance with international human rights standards and ensuring respect of all human rights, including the right to privacy;
- To underline the role and responsibilities of private actors, particularly surveillance companies, that transfer surveillance technologies to state actors with poor human rights records;
- To urge states take a human rights-centred approach in their use of these technologies, and ensure that their use is consistent with the right to privacy, including the protection of personal data;
- To urge states to avoid using the obligation to protect against enforced disappearances as a pretext to introduce broad and overreaching surveillance measures.

1. The use of new technologies to facilitate enforced or involuntary disappearances

Enforced disappearances constitute a serious violation of human rights and a grave threat to the rule of law and democratic principles. Privacy International is concerned that the use of new technologies, particularly those used for surveillance purposes, has further facilitated the commission of enforced disappearances by state actors. Various examples demonstrate the link between use of unprecedented surveillance capabilities and instances of enforced disappearance.

The report by Privacy International, "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism In Kenya", provides a detailed analysis of the connection between surveillance and enforced disappearances in Kenya.[2]

According to our findings, the Kenyan authorities have used a wide range of surveillance technologies, including cellular network interception, satellite imagery, and data analysis, to monitor the communications and movements of individuals. The authorities have used the information collected by these practices to target individual, often in the absence of due process or the rule of law. It further highlights the significant human rights violations that have resulted from these practices, including the disappearance and death of individuals who have been targeted by the Kenyan authorities.[3]

This report demonstrates how the use of surveillance in Kenya has facilitated enforced disappearances and highlights the importance of addressing this issue to protect the rights of individuals and the rule of law. The report concludes that the Kenyan authorities must take immediate action to review and reform their surveillance practices, hold those responsible for human rights violations accountable, and provide reparations to victims and their families.

The connection between surveillance and enforced disappearances has emerged in other countries too. For example, in the Xingjiang region of Western China, where surveillance is being used to facilitate the government's persecution of 8.6million Uighur Muslims.[4] It has been widely reported by UN bodies,

[2] PI, "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism In Kenya", March 2017, https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf
[3] *ibid.*
[4] PI, "Privacy matters because…it can protect us from being discriminated against", 12 December 2019, https://privacyinternational.org/case-study/3308/it-can-protect-us-being-discriminated-against

human rights groups and journalists how the Chinese government has been using advanced technologies, such as facial recognition and data analytics, to monitor and repress ethnic minorities, particularly Uighur Muslims in Xinjiang province.[5] This has led to a significant increase in the number of enforced disappearances in the region. There have been numerous reports over the past years over disappearances of Uighurs.[6]

Similarly, in Egypt, the government has been using surveillance technologies to track and detain individuals, including political opponents, journalists, human rights defenders and other individuals suspected of being critical of the government. Human Rights Watch reported that Egyptian authorities have used surveillance and technology to track and arrest human rights defenders and opposition figures.[7] One example is the case of Giulio Regeni, an Italian doctoral student who was researching trade unions in Egypt. He was disappeared and later found dead, with evidence of torture on his body. Following his death, it was reported that the Egyptian authorities had been monitoring his movements using new technologies.[8] Human rights groups, such as Amnesty International, have highlighted how this example is part of a wider pattern of enforced disappearances by intelligence agencies across Egypt.[9]

Worth noting that a French surveillance company, Nexa technologies (former Amesys)[10] is before French courts for having sold cybersurveillance equipment to President Al-Sisi's government in Egypt which would have enabled it to track down opponents in a case brought by two human rights groups – the International Federation for Human Rights (FIDH) and the French League for Human Rights (LDH).[11] The company was indicted in Paris in October 2021 for "complicity in acts of torture and of enforced disappearances" and case is ongoing. [12]

[5] OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China, 31 August 2022, https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf; Johana Bhuiyan, "'There's cameras everywhere': testimonies detail far-reaching surveillance of Uyghurs in China", 30 September 2021, https://www.theguardian.com/world/2021/sep/30/uyghur-tribunal-testimony-surveillance-china; Human Rights Watch, "How Mass Surveillance Works in Xinjiang, China", 2 May 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang

[6] Indicatively, Amnesty International, "China: Parents of missing Uyghur children describe horror of family separation", 19 March 2021, https://www.amnesty.org/en/latest/press-release/2021/03/china-parents-of-missing-uyghur-children-describe-horror-of-family-separation/; Ali MC, "Australia Uighurs despair over 'disappeared' relatives in China", AlJazeera, 4 June 2021, https://www.aljazeera.com/news/2021/6/4/uighurs-in-australia-struggle-to-contact-families-in-xinjiang; Austin Ramzy & Chris Backley, The Xinjiang Papers, The New York Times, 16 November 2019, https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html

[7] Most recently, Human Rights Watch, "Egypt: Detentions, Repression Follow Protest Calls", 16 November 2022, https://www.hrw.org/news/2022/11/16/egypt-detentions-repression-follow-protest-calls

[8] Ruth Michaelson & Stephanie Krichgaessner, "A year on, Giulio Regeni death casts shadow over Italy-Egypt relations", The Guardian, 25 January 2017, https://www.theguardian.com/world/2017/jan/25/giulio-regeni-death-italy-egypt-libya-cambridge-student

[9] Amnesty International, "Egypt: Hundreds disappeared and tortured amid wave of brutal repression", 13 July 2016, https://www.amnesty.org/en/latest/news/2016/07/egypt-hundreds-disappeared-and-tortured-amid-wave-of-brutal-repression/

[10] Nexa Technologies (includes company previously known as Amesys, or Advanced Middle East Systems) is a technology company that produces tools for intercepting communication and analysing data, as well as other information products.

[11] FIDH, "Vente de matériel de surveillance par Amesys à l'Egypte : l'impunité doit cesser", 5 July 2017, https://www.fidh.org/fr/regions/maghreb-moyen-orient/egypte/vente-de-materiel-de-surveillance-par-amesys-a-l-egypte-l-impunite

[12] Business & Human Rights Resource Centre, "French technology firm Nexa indicted for "complicity in torture and enforced disappearances" in Egypt and Libya", 29 November 2021, https://www.business-humanrights.org/en/latest-news/french-technology-firm-nexa-indicted-for-complicity-in-torture-and-enforced-disappearances-in-egypt-and-libya/

Mexico provides another example of a state where the relationship between new technologies and enforced disappearances has been a growing concern.[13] In recent years, Mexico has experienced a high rate of disappearances, with tens of thousands of individuals reported missing. The widespread use of new technologies, with use of spyware Pegasus being extensively covered, but also other technologies, by state actors has been criticized for facilitating the commission of these disappearances.[14]

One example is the case of the 43 students from the Ayotzinapa Rural Teachers College who disappeared in 2014.[15] The official investigation into their disappearance that was set up by the Inter-American Commission on Human Rights concluded that the Mexican authorities had been monitoring the students' communications and movements using new technologies.[16] The investigation also revealed evidence of collusion between state actors and organized crime groups in the commission of the disappearances. [17]

States need to ensure that the use of new technologies is in compliance with international human rights law, including the International Covenant on Civil and Political Rights (ICCPR) and the International Convention for the Protection of All Persons from Enforced Disappearance. The right to privacy as protected by Article 17 of the ICCPR, which states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation", and the right to life as protected by Article 6 of the ICCPR are also implicated and violated when unlawful surveillance practices are used to facilitate enforced disappearances.

The use of surveillance to facilitate enforced disappearances is a serious human rights concern that must be addressed by states individually and the international community. It is crucial that states take immediate action to review and reform their surveillance practices and hold those responsible for human rights violations accountable, and provide reparations to victims and their families. Furthermore, the Working Group on Enforced or Involuntary Disappearances have an important role to play in raising awareness about this issue and holding states accountable for their actions.

2. The normalisation of surveillance as a justification for complying with their obligations to take positive steps to protect people against enforced or involuntary disappearances

The widespread use of new technologies has the potential to enhance the ability of states to prevent and investigate enforced disappearances in accordance with their international human rights obligations. However, it is increasingly clear that some states are using the guise of protecting against enforced disappearances as a pretext to introduce broad and overreaching surveillance measures. Such measures have the potential to violate human rights, including the right to privacy and the right to life.

[13] Amnesty International, "Mexico 2021" Report, https://www.amnesty.org/en/location/americas/north-america/mexico/report-mexico/; Human Rights Watch, "Mexico Events of 2020", https://www.hrw.org/world-report/2021/country-chapters/mexico

[14] R3D, "Pegasus", https://r3d.mx/tag/pegasus/; PI, Amnesty International and Centre for Research on Multinational Corporations (SOMO), "Operating from the Shadows: Inside NSO Group's Corporate Structure" (2021) https://www.privacyinternational.org/report/4531/operating-shadows-inside-nso-groups-corporate-structure

[15] Inter-American Commission on Human Rights, "Situation of Human Rights in Mexico", Country Report, 2016, https://www.oas.org/en/iachr/reports/pdfs/Mexico2016-en.pdf

[16] Centro Prodh, "Informe GIEI Ayotzinapa III", 29 March 2022, https://centroprodh.org.mx/2022/03/29/informe-giei-ayotzinapa-iii/; Interdisciplinary Group of Independent Experts (GIEI), Reports, https://www.oas.org/en/IACHR/jsForm/?File=/en/IACHR/GIEI/Ayotzinapa/reports.asp

[17] *ibid.*

For example, the Inter-American Development Bank claimed that Jamaica's National Identification System (NIN) will help to better protect children "against kidnapping and child trafficking, which are on the rise worldwide".[18] In Mexico, a new law would have required cell phone companies to collect biometric data like fingerprints or eye scans from customers. The government justified this among others as a solution to help identify the disappeared.[19] The Mexico's Supreme Court struck down this law. In the process those that challenged the law raised the same in the reverse that the new measure would aid the kidnappers.[20]

ID systems can be used as tools of surveillance within a broader surveillance infrastructure, often leading to disproportionate and unnecessary interference with privacy and enabling violations of other human rights. In the most concerning cases, the data collected as part of digital ID systems scheme could be used to identify and target perceived opponents, as reported following the Taliban takeover of Afghanistan.[21]

Companies are playing a key role in marketing their surveillance tools as solutions to the process. For example, Clearview AI, an online surveillance company, had offered its services to the Ukrainian defense ministry to search among others for missing people.[22] Privacy International has expressed its concern about Clearview's partnership with Ukraine,[23] most notably in light of the fact that Clearview's data collection has been found in violation of many countries' privacy laws.[24]

Privacy International is concerned that broad, indiscriminate surveillance measures are introduced under the pretext of countering enforced disappearances and facilitate their investigations. First, quite often these surveillance powers are not compliant with international human rights law and standards.[25] Second, they are not often an effective solution to identifying the disappeared and they risk diverting resources of investigatory authorities, resources that are often scarce. Third, these surveillance measures increase the risk of the commission of grave human rights violations. As the examples in previous part of this submission have shown, the collection and use of data obtained through such surveillance measures has facilitated the commission of enforced disappearances and other human rights violations.

We respectfully recommend that the Working Group on Enforced or Involuntary Disappearances advise states to avoid using the obligation to protect against enforced disappearances as a pretext to introduce broad and overreaching surveillance measures. Instead, states should ensure that the use of new

[18] Inter-American Development Bank, "New IDB-supported national identity system in Jamaica to cut transaction costs, facilitate services", 8 December 2017, https://www.iadb.org/en/news/news-releases/2017-12-08/jamaica-national-identification-system-loan%2C12001.html

[19] Cassandra Garrison, "Kidnap capital Mexico eyes biometric phone registry, sparking privacy fears", 16 February 2021, https://www.reuters.com/world/china/kidnap-capital-mexico-eyes-biometric-phone-registry-sparking-privacy-fears-2021-02-16/

[20] "Mexican court strikes down cellphone personal data registry", Jamaica WI The Cleaner, 26 April 2022, https://jamaica-gleaner.com/article/world-news/20220426/mexican-court-strikes-down-cellphone-personal-data-registry

[21] Human Rights Watch, "New Evidence that Biometric Data Systems Imperil Afghans", 30 March 2022 https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans; PI, "Afghanistan: What Now After Two Decades of Building Data-Intensive Systems?", 19 August 2021, https://privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems

[22] Clearview AI, "Ukraine", https://www.clearview.ai/ukraine

[23] Privacy International, "The Clearview/Ukraine partnership - How surveillance companies exploit war", 18 March 2022, https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war

[24] In Europe only see Clearview AI, "Challenge against Clearview AI in Europe", https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe

[25] Privacy International's response to the call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights highlight the human rights concerns regarding surveillance measures as well as introduction of biometric identification systems. "Privacy International's response to the call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights", June 2022, https://privacyinternational.org/sites/default/files/2022-06/PI%20submission%20to%20OHCHR%202022%20report%20final.pdf

technologies is in compliance with international human rights law. Any measures taken to protect people from enforced disappearances should be understood and interpreted in light of other human rights obligations, such as the right to privacy and data protection.[26] This includes ensuring that any surveillance measures are in accordance with law, necessary and proportionate, and that strong safeguards and accountability mechanisms are in place to prevent the abuse of these technologies and to ensure that they do not facilitate the commission of human rights violations.

[26] See for example, Human Rights Center and UN OHCHR, "Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law", 2022; https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf