Access Now Submission to the United Nations Working Group on Enforced or Involuntary Disappearances for UN Human Rights Council 53rd Session Report on "New technologies and enforced disappearances"

3 February 2023

Introduction

Access Now welcomes this opportunity to provide relevant information to the United Nations (UN) Working Group on Enforced or Involuntary Disappearances (Working Group) to inform the thematic report on new technologies and enforced disappearances to be presented to the UN Human Rights Council at the 53rd session in June 2023.[1] Access Now, a UN Economic and Social Council (ECOSOC) accredited organization, routinely engages with the UN in support of our mission to extend and defend digital rights of people and communities at risk around the world.[2] Since its founding in 2009, Access Now has monitored the abuse and misuse of new and emerging technologies that threaten fundamental human rights, including freedoms of expression, association, and peaceful assembly, as well as the rights to privacy and non-discrimination.

This submission focuses on the use of targeted surveillance technologies, such as spyware, to facilitate enforced disappearances, in violation of international human rights law. It is important to note that, while this submission draws upon examples, these examples are non-exhaustive and do not represent the lived experiences of all persons at risk. More information is required to take into full account the intersecting forms of oppression of those who are directly targeted.

The use of spyware to facilitate enforced disappearances and hinder justice

1. Spyware[3] has repeatedly been used against human rights defenders, activists, journalists, lawyers, and political opponents worldwide. From authoritarian to democratic countries, the arbitrary and unlawful surveillance of organizations and individuals, including relatives of disappeared persons, yields damning impacts on democratic processes as well as on access to justice and remedy.

2. Families demanding the whereabouts of their loved ones often live in fear of reprisal if they seek the truth. They are often at increased risk of physical harm and reprisal by the perpetrators of the disappearance. Spyware magnifies these risks by allowing unrestricted access to their

[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.

[2] Access Now, About Us, 2021, available at https://www.accessnow.org/.

[3] Spyware is a form of malware that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting, or analyzing data from natural or legal persons' devices, in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data, or tracking activities across multiple end-user devices.

devices and data. The private and personal information that can be collected and delivered to the inflicting party can be weaponized to commit further abuses against families seeking justice, blackmail individuals into silence, or cause physical harm.

3. Among its many malicious purposes, spyware instills fear in affected users and deters them from taking action. Knowing that they may be targeted, with their every move being watched, and consequently putting themselves and other loved ones at risk, may be enough to scare families away from asserting their rights for fear of reprisal. Spyware also makes it more difficult for surveilled individuals to conduct investigations and prepare for legal proceedings in relation to the enforced disappearance, which requires safety and privacy.

    a. In 2021, Amnesty International confirmed the infection of a device belonging to [redacted] an imprisoned **Rwandan** activist and outspoken critic of the Kagame government. Since at least January of that year, [redacted] phone – and all of [redacted] communications, contacts, location, and more – were exposed by Pegasus[4] spyware. [redacted] was forcibly disappeared between August 27–31, 2020, until the Rwanda Investigation Bureau (RIB) disclosed [redacted] was in their custody.[5] The family, however, was not able to speak to [redacted] until September 8 of that year. [redacted] [The activist] was later sentenced under unfounded terrorism charges to be imprisoned for 25 years. Since his disappearance and imprisonment, [redacted] has been fearlessly leading her family's efforts to seek the truth. [redacted]'s infection suggests that the Kagame government – which has long been suspected of being a client of the Israeli surveillance firm NSO – has been able to monitor her private calls and discussions with U.S., European, and British government officials as part of her efforts to deliver justice [redacted]. While the Rwandan government denies these allegations, the evidence suggests that [redacted] was targeted in an effort to stop the [redacted]s activism over the case.

    b. Similarly, in 2017, The Citizen Lab confirmed that the Group of Independent Experts (GIEI) investigating the **Mexican** government's possible involvement in the 2014 Iguala Mass Disappearance were targeted with attempts to infect their devices with Pegasus spyware.[6] These infection attempts came alongside a campaign of harassment and criticism by allies of the government – an illustration of how spyware can be used to interfere with investigations of enforced disappearances.

---

[4] Pegasus is a spyware developed by the notorious Israel-based company NSO Group. In 2021, The Pegasus Project, led by Amnesty International and Forbidden Stories, uncovered how governments worldwide were using NSO Group's invasive Pegasus spyware to put human rights activists, political leaders, journalists, and lawyers around the world under unlawful surveillance, available at: https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/, 2021.

[5] Human Rights Watch, Rwanda: [redacted] Was Forcibly Disappeared, available at: https://www.hrw.org/news/2020/09/10/rwanda-rusesabagina-was-forcibly-disappeared , September 10, 2020.

[6] The Citizen Lab, Reckless II, Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware, available at: https://citizenlab.ca/2017/07/mexico-disappearances-nso/ , July 10, 2017.

4. A successful infection of a target's phone by spyware may give the perpetrator valuable information on the target's whereabouts, activities, contacts, and data that can help track, trace, and locate individuals in order to forcibly disappear them. It allows states to surveil and locate targets.

5. The disappearance and then extrajudicial execution of [redacted], **Saudi** journalist and dissident, illustrates how spyware can be used to facilitate further human rights violations including enforced disappearance and extrajudicial killing. Prior to [redacted]'s execution on October 2, 2018, at the Consulate of the Kingdom of Saudi Arabia in Istanbul, a number of his family members and acquaintances were targeted by Pegasus spyware.

    a. Investigations by Amnesty International, The Citizen Lab, and the Washington Post showed that [redacted], was targeted with Pegasus spyware between November 2017 and April 2018, just after she had gotten engaged to Khashoggi.[7]

    b. The phone of [redacted]'s close associate [redacted] was also infected with Pegasus while he was in regular contact with [redacted] just several months before his death.[8]

    c. A number of [redacted]s brothers, relatives, and friends were also arrested in Saudi Arabia during that period, which he believes happened after his phone was hacked.[9] This suggests that data gathered during the infection could have been used to track down [redacted] and plan for his extrajudicial killing, which, according to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, was premeditated.[10]

    d. [redacted] was also targeted with Pegasus just four days after his murder, on 6 October 2018 and on two other days in October 2018.[11]

---

[7] The Washington Post, A UAE agency put Pegasus spyware on phone of [redacted] before his murder, new forensics show, 21 Dec 2021, available at https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus.

[8] The Citizen Lab, The Nso Connection To [redacted], 24 Oct. 2018, https://citizenlab.ca/2018/10/the-nso-connection-to-jamal-khashoggi.

[9] The Guardian, [redacted] 'I'm worried about the safety of the people of Saudi Arabia', available at:https://www.theguardian.com/film/2021/feb/20/me[redacted]

[10] Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Investigation of, accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents, 4 Oct 2019, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/296/91/PDF/G1929691.pdf?OpenElement.

[11] The Guardian, Saudis behind NSO spyware attack on [redacted] leak suggests, 18 July 2021, available at https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-[redacted]

e. It is also suspected that the phones of [redacted],[12] [redacted],[13] and officials investigating his murder had been targeted.[14] Furthermore, reports indicate that a number of [redacted]'s friends, including [redacted] were identified as potential targets by NSO Group's government clients.[15] This would suggest an intention to interfere in the investigation, and silence relatives and loved ones from seeking justice and accountability.

6. On 13 March 2018, [redacted], a Saudi women human rights activist, was kidnapped in the United Arab Emirates (UAE) while driving on the highway and flown back to Saudi Arabia in a private jet, where she was detained until her release on March 15, 2018. On May 15, 2018, [redacted] was re-detained,[16] and seven days later, transferred to a secret prison in Jeddah, where she was subject to interrogation and torture. A 2019 Reuters investigation revealed that [redacted] was targeted in 2017 by a team of U.S. mercenaries who surveilled dissidents on behalf of the UAE under a program called Project Raven,[17] which categorized her as a national security threat and hacked her iPhone before she was arbitrarily detained in the UAE. Evidence suggests that [redacted] infection with DarkMatter[18] spyware led to her arbitrary arrest by the UAE's security services and rendition to Saudi Arabia, where she was detained, imprisoned, and tortured. [redacted] is currently suing DarkMatter Group and three of its former executives "for illegally hacking her iPhone to secretly track her communications and whereabouts."[19]

7. In August 2016, Citizen Lab findings showed that [redacted], a renowned Emirati human rights activist, was targeted with three different surveillance products, including FinFisher's Finspy spyware in 2011 and Hacking Team's Remote Control System in 2012. In 2016, he was targeted by Pegasus.[20] Project Raven also hacked Mansoor's device in 2016, and a year later, [redacted].[21] [redacted] was initially jailed for a period of eight months in 2011 after calling for greater

---

[12] Haaretz, [redacted]nvestigation Reveals, 18 July 2021, available at https://www.haaretz.com/israel-news/tech-news/2021-07-18/ty-article/.premium/[redacted]

[13] BBC, Pegasus: Who are the alleged victims of spyware targeting? 22 July 2021, https://www.bbc.com/news/world-57891506

[14] The Washington Post, [redacted]With Spyware Before His Death, July 18, 2021, available at: https://www.washingtonpost.com/investigations/[redacted]

[15] Yasin Aktay Profile, available at: https://cdn.occrp.org/projects/project-p/?_gl=1*x8nyel*_ga*MjAzODA5NzU5My4xNjc1NDI2ODI5*_ga_NHCZV5EYYY*MTY3NTQyNjgyOC4xLjAuMTY3NTQyNjgyOC42MC4wLjA.#/profiles/192

[16] *See* Loujain AlHathloul, https://www.loujainalhathloul.org/arrest-torture-charges.

[17] Reuters, Project Raven, available at: https://www.reuters.com/investigates/section/usa-raven/ , January 20, 2019

[18] *Ibid.*

[19] Electronic Frontier Foundation, Saudi Human Rights Activist, Represented by EFF, Sues Spyware Maker DarkMatter For Violating U.S. Anti-Hacking and International Human Rights Laws, available at: https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating, December 9 2021.

[20] The Citizen Lab, The Million Dollar Dissident, available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, August 24, 2016

[21] Electronic Frontier Foundation, alHathloul Vs DarkMatter, available at: https://www.eff.org/document/alhathloul-v-darkmatter, September 12, 2021.

political rights and freedoms.[22] In March 2017, UAE security forces raided [redacted]'s home and arrested him again. For more than a year following his arrest, [redacted]'s family members did not know his whereabouts, and he had no access to a lawyer. In May 2018, he was sentenced to 10 years in prison[23] under vague charges of "insulting the status and prestige of the UAE and its symbols, including its leaders," "publishing false information to damage the UAE's reputation abroad," and "portraying the UAE as a lawless land."[24] Evidence suggests that the UAE government is the likely operator behind [redacted]s targeting.[25]

8. These cases demonstrate the adverse impacts that targeted surveillance tools, such as Pegasus spyware, can have on individuals. Moreover, according to Human Rights Watch, such surveillance not only affects the directly targeted victims; it also has a chilling effect on the victims' family members as well as other human rights defenders, such as advocates or journalists, who – knowing their family members or colleagues are being surveilled – start to self-censor because they are afraid they might also be targeted.[26] Additionally, journalistic sources and witnesses to crimes might be afraid to speak up out of fear of being surveilled.[27]

Legal Framework

9. The opaque surveillance technology industry has long been left to facilitate human rights abuses and operate without scrutiny. Few laws and mechanisms meaningfully restrict the trade, development, and use of surveillance technology at the national and international levels. The use of such technology is often justified under vague and ill-defined national security laws. Given the secrecy and lack of accountability in crimes such as enforced disappearances, it is all the more difficult to ensure enforcement of applicable laws in such cases in particular. However, some efforts have been made to rein in surveillance technologies.

    a. In 2013, **Wassenaar Arrangement (WA) member states** agreed to implement a multilateral export regime on "Intrusion Software" and "IP Network Surveillance Systems,"[28] in an attempt to address the proliferation of spyware.[29] However, the

[22] Human Rights Watch, UAE: Free Activists Before Elections, available at: https://www.hrw.org/news/2011/09/22/uae-free-activists-elections, September 22, 2011

[23] Human Rights Watch, The Persecution of [redacted] available at: https://www.hrw.org/report/2021/01/27[redacted] January 27, 2021

[24] Gulf Center for Human Rights, Open Letter to the Emirati Authorities, available at: https://www.gc4hr.org/news/view/2229, October 16, 2019

[25] The Citizen Lab, The Million Dollar Dissident, available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, August 24, 2016

[26] Human Rights Watch, 'Spyware Used to Hack Palestinian Rights Defenders: Groups Condemn Use of NSO Group's Pegasus Against Palestinians' (November 8, 2021) available online at: https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders.

[27] Human Rights Watch, 'Unchecked Spyware Industry Enables Abuses: Governments Should Halt Trade in Surveillance Technology', July 30, 2021, available online at: https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses.

[28] Access Now, Considerations on the Wassenaar Arrangement, available at: https://www.accessnow.org/cms/assets/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf, 2015

[29] See, e.g. Privacy International, US Publishes Proposed Rules Implementing 2013 Wassenaar Agreements, 28 May 2015, available at

agreement is non-binding, and member states have not shown much enthusiasm in adopting such export controls, or instituting stronger safeguards that take into account human rights concerns associated with the use of spyware. Whatever the intentions of those engaged in the Wassenaar process, the past decade of abuses and consistent revelations of the trade and unlawful use of surveillance technologies – often involving WA member states – demonstrates that the current regime is not fit for purpose, and fails to put human rights at the center of its concerns. Advocates look to the development of the Export Controls and Human Rights Initiative,[30] launched at the U.S. Summit for Democracy in 2021, as an important new step that bridges the intimate relationship between spyware export and human rights abuses.

b. In March 2021, the **European Union** adopted the recast Dual Use regulation, which aimed at preventing human rights harm resulting from digital surveillance by establishing controls for surveillance technology exported by E.U.-based companies.[31] While a positive development, the agreement falls short of providing explicit and strong conditions on E.U. Member State authorities and exporters.[32]

c. In November 2021, the **United States** government added NSO and Candiru to its U.S. Commerce Department Entity List for engaging in activities contrary to the national security or foreign policy interests of the United States.[33] The U.S. Congress took additional steps to help combat spyware in December 2022, by including several measures and restrictions on foreign commercial spyware in its 2023 National Defense Authorization Act.[34] While primarily aimed at creating protections for U.S. intelligence community personnel, it could also generate new avenues to address the use of spyware around the world by promoting international governmental coordination.

10. National and regional data protection laws could also be relevant in the regulation of the use of spyware. However, given the exponential proliferation of this industry despite ample evidence of its harms and threats to human rights as a tool of transnational repression, it is time for an international framework with wider commitment to govern its use.

---

https://privacyinternational.org/blog/1425/us-publishes-proposed-rules-implementing-2013-wassenaar-agreements.

[30] The White House, Export Controls and Human Rights Initiative launched at the Summit for Democracy, available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/, December 10, 2021

[31] Access Now, New EU dual use export control rules finally adopted, but leave a lot of room for improvement, available at: https://www.accessnow.org/eu-dual-use-export-control-rules-room-for-improvement/, March 25, 2021

[32] Access Now, Human Rights Organizations Response to the Adoption of the New EU Dual Use Export Control Rules, available at: https://www.accessnow.org/cms/assets/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf, March 2021

[33] US Department of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, 3 Nov. 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[34] Access Now, U.S. Congress takes additional steps to combat spyware, December 23, 2022, available at: https://www.accessnow.org/spyware-ndaa-2023/,

Investigation and Prosecution

11. The secrecy surrounding crimes of enforced disappearances, topped by the opaque nature of the spyware industry and lack of regulatory laws and mechanisms, makes it all the more challenging for rights holders to find effective avenues to seek justice and remedy. However, in one successful example in November 2022, after more than 10 years since the lodge of the complaint by the International Federation for Human Rights and the French Human Rights League, the Investigative Chamber of the Paris Court of Appeal confirmed the indictment of a surveillance company formerly known as Amesys, now Nexa Technologies, and its executives. The complaint detailed "the company's sale of surveillance software to authoritarian regimes in Libya and Egypt that resulted in torture and disappearance of dissidents."[35]

Conclusion and recommendations

1. **To states:**
    a. Implement an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards are put in place to regulate such practices;
    b. Establish a legal and policy framework – at national and international levels – that makes the acquisition of surveillance tools subject to robust public oversight, consultation, and control, in order to comply with safeguards against illegitimate access, and to guarantee the principles of necessity, proportionality, legality, legitimacy, and due process, in accordance with the 13 Principles on the Application of Human Rights to Communications Surveillance[36];
    c. Recognize and enforce the right to remedy and reparation through strong and independent oversight measures for individuals targeted by cyberespionage;
    d. Hold companies that develop and distribute these technologies accountable for their failure to respect human rights and to acknowledge their contributions to abusive end uses, and demand transparency from said companies around the extent of data obtained and their processing;
    e. Review and reform all relevant laws and regulations governing the import, export, procurement, development, oversight, sale, transfer, servicing, and use of targeted surveillance technologies in order to ensure compliance with international human rights law and norms;
    f. Develop and encourage the adoption of robust safeguards and standardized clauses in any contract of purchase and sale of cyber surveillance programs to ensure compliance with human rights standards for any use of these products and services;

[35] International Federation For Human Rights, Surveillance and torture in Libya: The Paris Court of Appeal confirms the indictment of Amesys and its executives, and cancels that of two employees, November 21, 2022, available at: https://www.fidh.org/en/impacts/Surveillance-torture-Libya-Paris-Court-Appeal-indictment-AMESYS

[36] Necessary and Proportionate Principles, https://necessaryandproportionate.org/principles.

g. Identify those involved in the spyware trade, including sellers, transshippers, affiliates, financiers, and clients, and take measures to prevent their acquisition, transfer, financing, and procurement of spyware, including through targeted sanctions; and
h. Publicly report any detected misuse of cybersurveillance products and services resulting in human rights violations to any relevant oversight body, either at the national, regional, or international level.

2. To the private sector, including both companies and their investors:

a. Commit publicly to the implementation of the U.N. Guiding Principles on Business and Human Rights (UNGPs);
b. In line with the UNGPs, publicly affirm a commitment to respect all fundamental rights by putting in place a human rights policy covering all areas of the business;
c. Put in place policies and practices that identify, assess, and address the impact of the business on human rights, including appropriate consideration for business partners and customers, as well as high-risk individuals and communities who may be impacted by the company's products or operations, and potential impact of technology misuse;
d. Create and implement a strategy to push back on government or law enforcement assistance requests which appear overbroad, unlawful, or disproportionate, and publicly report on the requests you received and how you responded;
e. Engage with peers and stakeholders, including civil society, to verify the governance put in place to mitigate the potential adverse human rights impacts is effective and appropriate;
f. Issue regular public reports on the related due diligence efforts and procedures in place to cease, prevent, and mitigate negative human rights impacts; and
g. Put in place a grievance mechanism to ensure access to remedy from potentially affected stakeholders.

3. To international organizations:

a. Highlight the abuse of spyware, through interventions and resolutions at the Human Rights Council, General Assembly, and other U.N. fora;
b. Engage with the Office of the High Commissioner for Human Rights and Special Procedures to monitor, maintain pressure, and ensure U.N. action on the matter;
c. Take concrete steps to ensure independent and accessible legal avenues for complaints, both domestically and internationally, are available for victims of spyware, including those in relation to an enforced disappearance; and
d. Join civil society's efforts in pushing for strict regulation of the spyware industry.
e. In particular, to the **Working Group on Enforced or Involuntary Disappearances**:
    i. Highlight the role of spyware in perpetrating human rights abuses, including its facilitation of enforced disappearance and obstruction of justice, in upcoming reports and meetings with states, and condemn the abuse of spyware by states;

ii. Join other Special Procedures in calling for a moratorium[37] on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards are put in place to regulate such practices; and

iii. Facilitate the filing of individual Complaints involving the intersection of surveillance technologies and enforced disappearances, and issue Communications to States responsible.

Access Now (https://www.accessnow.org) defends and extends the digital rights of people and communities at risk around the world. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact: **un@accessnow.org***

[37] OHCHR, Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech, 12 August 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.