Freedom House

Social Media Surveillance and Spyware as Tools in the Perpetration of Transnational Repression and Enforced Disappearances

This submission will focus on the first key issue raised by the working group, namely, "How new technologies are being used against relatives of disappeared persons, their representatives, human rights defenders and civil society organizations, and which kind of protective strategies are – or can be put – in place."

In particular, this submission concentrates on **the issue of new technologies in transnational repression and the intersection with enforced disappearances**.

Transnational repression[1] encompasses cross-border acts of intimidation, violence, and harassment. It is not intended to describe a new or discrete form of human rights violation, but rather violations of a uniquely transnational nature because they are perpetrated by one state in the national jurisdiction of another. As such, acts of transnational repression have specific legal, social, and political characteristics distinct from human rights violations committed by a government within its own jurisdiction.

"New technologies" as used in the broad sense by the Working Group are crucial to the growth of transnational repression globally.

First, new technologies themselves are mechanisms *for* transnational repression, in that digital threats and digital surveillance themselves can have a silencing effect upon diasporas and exiles. States use ICTs to conduct intimidation and harassment campaigns across national borders. These digital threats encompass relatives and representatives of disappeared persons, as well as human rights defenders and civil society organizations. These digital transnational repression campaigns can have significant impact on the health and well-being of the individuals targeted, and may deter them from continuing their work. The personal nature of digital communications, particularly via mobile devices, makes threats via those communications highly significant for individuals. Disseminating personalized, bodily threats against people seeking justice for a disappeared person is a cheap, anonymous, and effective way for states to intimidate advocates. As scholar Marcus Michaelsen has written, "Targeted activists experience constant tension and stress, and see their ties to the home country undermined. In turn, the dynamics, impact, and outreach of diaspora activism are inevitably altered. These practices of transnational repression represent deliberate and systematic interferences in the fundamental

[1] Nate Schenkkan and Isabel Linzer, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression,* Freedom House, February 2021, https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf

human rights of the targets, primarily by violating their right to privacy and freedom of expression." [2]

Second, new technologies provide unprecedented opportunities for surveillance, which in turn can enable other human rights violations, including enforced and involuntary disappearances. ICTs that facilitate communication across borders also facilitate surveillance of those communications and other personal data. States collect such information by monitoring public platforms as well as by conducting targeted surveillance.

Monitoring platforms like Facebook, Twitter, or Telegram provides a diagram of social connections that can be useful to intelligence services seeking to understand the activities of exile or diaspora activists and journalists. Such **social media surveillance** is highly valuable for tracing how a community organizes, shares information, and collaborates. In 2019, Freedom House found that 40 of the 65 countries covered in its *Freedom on the Net* report conducted social media surveillance.[3] While not all these programs require advanced technical skills, governments are increasingly deploying automated technology for monitoring platforms, allowing for the real-time aggregation, organization, and analysis of large amounts of metadata and content in order to map people's networks, infer their location, and identify other patterns of activity. Social media surveillance has a chilling effect on freedoms of speech, assembly, and association, and it can lead to severe human rights violations.

Such surveillance plays a role in physical acts of transnational repression. In recent years, there has been a growth in cases of individuals imprisoned for online speech. This can include individuals who are reached transnationally, such as the American citizen [redacted], who was detained in Dubai in December 2022 after he criticized Egypt's president online.[4] In August 2022, a Saudi student at Leeds University in the United Kingdom was imprisoned upon returning to Saudi Arabia for critical tweets that she had sent while abroad.[5] In another representative case, in December 2019 the Azerbaijani-origin blogger [redacted] was stripped of his Russian citizenship and deported from Russia to Ukraine, whereupon he was again deported to Azerbaijan.[6]

States also seek access to individuals' location, contacts, communications, and other personal information that is accessible via their private electronic devices such as smartphones and computers. This information is highly valuable for states seeking to silence that person or their

---

[2] Marcus Michaelsen, *Silencing Across Borders: Transnational repression and digital threats against exiled dissidents from Egypt, Syria, and Iran,* Hivos, 2020, https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf

[3] Adrian Shahbaz and Allie Funk, *Social Media Surveillance*, Freedom House, 2019, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

[4] "U.S. citizen held in UAE after criticising Egypt president released, says fiancée," *Reuters*, 23 December 2022, https://www.reuters.com/world/us-citizen-held-uae-after-criticising-egypt-president-released-says-fiance-2022-12-23/

[5] Stephanie Kirchgaessner, "Saudi woman given 34-year prison sentence for using Twitter," *The Guardian,* 16 August 2022, https://www.theguardian.com/world/2022/aug/16/saudi-woman-given-34-year-prison-sentence-for-using-twitter

[6] "Ukraine: Azerbaijani Activist Deported on Politically Motivated Grounds," Freedom House, 15 December 2019, https://freedomhouse.org/article/ukraine-azerbaijani-activist-deported-politically-motivated-grounds

network. **Hacking campaigns that penetrate individual devices and install spyware,** or software that can be remotely deployed to collect information from a user's device without their consent, therefore have become a standard part of suppression of activism and journalism.

Spyware is frequently used a ainst the tar ets of transnational repression and their acquaintances. The circle of [redacted] was penetrated by the NSO Group's Pegasus spyware prior to his murder in the Saudi consulate in Istanbul in 2018.[7] Pe asus was also used to infiltrate the phone of [redacted] around the time he was kidnapped from Dubai by Rwandan officials and imprisoned.[8] Testifying before the U.S. Congress in 2022, [redacted] said that due to the Pegasus deployment against her she had "lost all sense of security in my private actions and my physical surroundings."[9]

Spyware and social media surveillance technologies are sold by private companies to states with minimal oversight and regulation.[10] This unregulated market has allowed extremely powerful tools to proliferate and placed them within the reach of all states globally, substantially widening the scope of who may be targeted.[11] The relatively low cost, and the ease of transnational deployment of social media surveillance and spyware, make these tools highly sought after by states engaging in transnational repression.[12]

As former Special Rapporteur for Freedom of Expression David Kaye has written with Marietje Schaake, the commercialization of spyware has brought us to "the precipice of a global surveillance tech catastrophe."[13] We note with approval *The right to privacy in the digital age* report by the Office of the High Commissioner for Human Rights, which recommends "moratoriums on the domestic and transnational sale and use of surveillance systems, such as hacking tools and biometric systems that can be used for the identification and classification of individuals in public places, until adequate safeguards to protect human rights are in place."[14]

---

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

[8] Stephanie Kirchgaessner, "[redacted] laced under Pe asus surveillance " *The Guardian,* 19 July 2021, https://www.the uardian.com/news/2021/jul/19 [redacted]

[9] "Statement of [redacted], July 27, 2022," Permanent Select Committee on intelligence – Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware," https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-KanimbaC-20220727.pdf

[10] Mark Mazzetti, Ronen Bergman, and Matina Stevis-Gridneff, "How the Global Spyware Industry Spiraled Out of Control," *The New York Times,* 8 December 2022, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html

[11] Steven Feldstein and Brian Kot, "Global Inventory of Commercial Spyware & Digital Forensics," Carnegie Endowment for International Peace, 11 January 2023, https://carnegieendowment.org/programs/democracy/commercialspyware

[12] Nicole Perlroth, "How Spy Tech Firms Let Governments See Everything on a Smartphone," 2 September 2016, https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html

[13] David Kaye and Marietje Schaake, "Global spyware such as Pegasus is a threat to democracy. Here's how to stop it." *The Washington Post*, 19 July 2021, https://www.washingtonpost.com/opinions/2021/07/19/pegasus-spyware-nso-group-threat-democracy-journalism/

[14] United Nations High Commissioner for Human Rights, *The right to privacy in the digital age,* 4 August 2022, A/HRC/51/17, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

We affirm that such safeguards are wholly lacking either at a domestic or a global level, and that moratoriums would therefore be appropriate.

When faced with these threats, what are protective strategies?

Digital hygiene refers to tools and practices that can improve the baseline level of security for an individual user, just as consistent dental hygiene improves oral health. This can include better practices like strong, randomized passwords; two-factor authentication; password managers; use of virtual public networks (VPNs), and end-to-end encrypted communications. Activists, human rights defenders, and family members of targeted individuals should all have access to free, high-quality digital hygiene trainings tailored to their needs.

The onus should not and cannot be on individuals to protect themselves against malicious state actors, however. There are severe limits to what digital hygiene can accomplish. For one, social media surveillance is still effective even if activists take perfect precautions. Activism in the digital age requires that activists be public and open about their activities on digital platforms, such as social media and messenger applications. But it is this very openness that enables their persistent surveillance online. Second, in a world where states have access to sophisticated spying tools, including "zero-click" hacks that do not even require a user to click on them to penetrate a device, digital hygiene is not a guarantee against infiltration.[15]

Beyond digital hygiene, therefore, stopping the proliferation of spyware and social media surveillance will require cutting off the supply of these tools through stiff export controls, a multilateral regime of sanctions, and halts to the sale and distribution of commercial versions of the technologies. It will also require stronger legal safeguards and regulation outlining under what circumstances surveillance can or cannot be justified, and opportunities for redress and accountability for improper use, including via judiciaries in host states of those targeted. In the digital age, stopping enforced disappearances—including those of a transnational nature—requires stopping the proliferation of tools of mass and targeted surveillance.

[15] Yana Gorokhovskaia and Isabel Linzer, *Defending Democracy in Exile: Policy Responses to Transnational Repression,* Freedom House, June 2022, https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf